UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TEXAS
BEAUMONT DIVISION

Peter Harris and Loni Harris, *Plaintiffs*, v. Upwintrade.com, a business association; David Shamlian, an individual; John Does 1 – 20, *Defendants*.	Case No. 1:24-cv-00313 **Affidavit of Evan Cole**

I, Evan Cole, state and swear as follows.

I. Introduction

1. My name is Evan Cole. I am of sound mind and capable of making this Affidavit. I have personal knowledge of the facts stated herein.

2. I am the founder of Digital Investigations, LLC. I am experienced in blockchain investigations and am knowledgeable about the pig-butchering scam epidemic and the tactics of cybercriminals like the Defendants in this case. I hold the Chainalysis Cryptocurrency Fundamentals and the Chainalysis Reactor Certifications.

II. Pig-Butchering Scams

3. I have reviewed the Plaintiffs' Verified Complaint, their Motion for *Ex Parte* Temporary Restraining Order and Expedited Discovery (the "Motion"), and relevant evidence described below. I have concluded that the Plaintiffs were the victims of what is known as a "pig-butchering scam." This is a type of cybercrime that has proliferated in recent years. I have reviewed Section III(A) of the Motion, which sets out background related to the pig-butchering epidemic. Based on my training and experience, I verify that the statements set out there are true and correct.

4. The method of initial contact, style of communications, deceptive tactics, and the nature of the 'trading platform' used by the Defendants show that this was a pig-butchering scam. I have attached the following publicly available materials for comparison to the facts of this case:

a. Exhibit 1-A is a ProPublica article titled *What's a Pig-Butchering Scam?*, which describes in detail the tactics used by scammers, which map directly on to the facts of this case.

b. Exhibit 1-B is a Secret Service bulletin titled *Cryptocurrency Investment Scams*, which includes a list of "Warning Signs," al-most all of which of which were present in this case.

c. Exhibit 1-C is an excerpt from the Federal Bureau of Investigation's Internet Crime Complaint Center's *2023 Internet Crime Report*, which shows that investment scams are the largest source of reported losses of any internet crime.

d. Ex. 1-D is an excerpt from *How Do Crypto Flows Finance Slav-ery? The Economic of Pig Butchering*, a 2024 academic paper that studied the pig-butchering epidemic.

e. Exhibit 1-E is a Reuters article titled *Crypto Scam: Inside the Billion-Dollar Pig-Butchering Industry*, which describes the organization, management, and tactics of the criminal syndicates that operate pig-butchering scams.

5. Comparison of these news reports, articles, and law-enforcement bulletins to the allegations in the Harrises' Complaint shows that this case bears all the classic signifiers of a pig-butchering scam. Based on my training and experience, I have concluded beyond any doubt that the Harrises were the victim of just such a scam perpetrated by the Defendants.

III. Blockchain Background

6. I have reviewed Section III(C) of the Motion, which explains blockchain technology, blockchain-tracing methodologies, and crypto-asset recovery methods. Each of the statements in Section III(C) is accurate, to the best of my knowledge and experience.

IV. Blockchain Tracing

7. I have reviewed Section III(D) of the Motion, which sets out information about the blockchain tracing of the assets stolen from the Plaintiffs. I verify that the statements set out there are true and correct.

8. Exhibit 1-F is a true and correct copy of a graph showing the tracing of the assets stolen from the Harrises to the Target Accounts

identified in the Motion. This graph was generated using Chainalysis Reactor, a leading blockchain-analytics software.

9. At its leftmost edge, the graph reflects transactions in which the Harrises sent cryptocurrencies with collective transfer-date value of $665,971.94 to addresses controlled by the Defendants. The circles labeled "Upwintrade Receiving Address" are the addresses to which the operators of the Upwintrade platform instructed Plaintiffs to transfer their assets.

10. Continuing to the right, each circle represents a distinct block-chain address. The lines between the circles show the flow of funds from one address to another. At the graph's right edge, there are four circles labeled "Remitano," "Revolut," "Bybit," and "Binance" (the "Receiving Exchanges"). These are the exchange-associated-address clusters to which the Harrises' stolen assets were ultimately transferred.

11. To ensure that only assets traceable to the Harrises were captured in my analysis, I filtered the transactions directed to the Receiving Exchanges by date, capturing only those transactions that occurred *after* the Harrises' assets arrived at the address that later transferred those assets to the relevant Receiving Exchange. I then exported a ledger of those transactions. A true and correct copy of this ledger is attached hereto as Exhibit 1-G.

12. Based on the evidence described above and on my training and experience, I have concluded that the accounts associated with the

transactions detailed in the transaction ledger attached as Exhibit 1-G are likely controlled by the Defendants and either hold or have held the Harrises' stolen assets and other proceeds of criminal activities.

13. As explained in the Motion, it is very easy to move cryptocurrencies on the blockchain. Crypto assets can be moved in seconds from address to address, or exchange to exchange. Based on my experience, if the Target Accounts are not frozen, it is likely the individuals who stole the assets held there will move them to a non-compliant exchange or a self-custody address, which would prevent the Harrises from recovering the assets stolen from them, thereby causing significant and irreparable harm.

V. Subpoena Targets

14. I have performed an "open-source intelligence" investigation in this matter in addition to the blockchain investigation described above. Open-source intelligence refers to publicly available information available about a subject, often technological in nature.

15. The Harrises set out their proposed subpoena targets in the Motion at Section IV(B)(1). I have attached evidence showing the connection of each of these subpoena targets to this case as follows.

Subpoena Target	*Connection to Case*	*Evidence*
Microsoft Corporation	Microsoft owns Skype, the messaging app that Shamlian primarily used to communicate with the Harrises.	Exhibit 1-H
Meta Platforms, Inc.	Meta owns Facebook, where the deception at issue in this case began	Exhibit 1-I

	and where the Harrises communicated with the defendants.	
SRS AB	SRS AB is the domain registrar for Upwintrade.com.	Exhibit 1-J
Mastercard Inc.	A "built-with" search of Upwintrade.com shows that, at some point, a Mastercard payments processing tool was installed on the site.	Exhibit 1-K
Visa Inc.	A "built-with" search of Upwintrade.com shows that, at some point, a Mastercard payments processing tool was installed on the site.	Exhibit 1-K
Data Room, Inc.	Data Room provided the U.S.-based servers from which the Defendants operated upwintrade.com.	Exhibit 1-J
LLC Technology Distribution Ltda	This entity owns and operates JivoChat, a live-chat plugin that the Defendants used to communicate with victims on Upwintrade.com.	Exhibit 1-L
Wild West Domains, LLC	This entity is the domain registrar for davidshamlian.com, the personal website of David Shamlian.	Exhibit 1-M
OrangeHost LLC	This entity provides web-hosting services for davidshamlian.com.	Exhibit 1-M
Elementor Ltd.	The Defendants used the Elementor site-building tool to build the website at davidshamlian.com.	Exhibit 1-N
Binance, Ltd.	A significant portion of the Bitcoin that the Defendants stole from the Harrises was ultimately deposited in accounts at the Binance cryptocurrency exchange.	Exhibit 1-F

Revolut Technologies, Inc.	A significant portion of the Bitcoin that the Defendants stole from the Harrises was ultimately deposited in accounts at Revolut, which is a "neo-bank" that offers both crypto- and fiat-denominated accounts.	Exhibit 1-F
Babylon Solutions Limited	This entity owns and operates the peer-to-peer cryptocurrency exchange Remitano. A significant portion of the Bitcoin that the Defendants stole from the Harrises was ultimately transferred to Remitano accounts.	Exhibit 1-F
Bybit Fintech Limited	A significant portion of the Bitcoin that the Defendants stole from the Harrises was ultimately deposited in accounts at the Bybit cryptocurrency exchange.	Exhibit 1-F

16. For the reasons set out in the table above, each of the Harrises' proposed subpoena targets are likely to be in possesssion of biographical, contact, payments, and/or account-activity information about the Defendants. Businesses like those operated by the proposed subpoena targets typically maintain such information in databases that allow for straightforward data isolation and export, such that the burden of providing the information requested by the Harrises will be minimal.

[SIGNATURE PAGE FOLLOWS]

VERIFICATION

I, Evan Cole, hereby verify and declare under penalty of perjury that the foregoing is true and correct.

Commonwealth of Virginia
County of Chesterfield

ıe foregoing instrument was acknowledged before me
on 07/30/2024 by Evan Cole.

ɔtarized remotely online using communication technology via Proof.

Evan Cole
Founder & Investigator
Digital Investigations, LLC
evan@digitalinvestigations.co

Dated: 07/30/2024

Exhibit 1-A

PROPUBLICA

What's a Pig Butchering Scam? Here's How to Avoid Falling Victim to One.

Thousands have lost huge sums after being lured into fraudulent online investment schemes by seemingly attractive strangers who strike up online conversations with them. Here's a guide to spotting the telltale signs.

Tara Anand, special to ProPublica

by Cezary Podkul

Sept. 19, 2022, 3:50 p.m. EDT

ProPublica is a nonprofit newsroom that investigates abuses of power. Sign up to receive our biggest stories as soon as they're published.

If you're like most people, you've received a text or chat message in recent months from a stranger with an attractive profile photograph. It might open with a simple "Hi" or what seems like good-natured confusion about why your phone number seems to be in the person's address book. But these messages are often far from accidental: They're the first step in a process intended to steer you from a friendly chat to an online investment to, ultimately, watching your money disappear into the account of a fraudster.

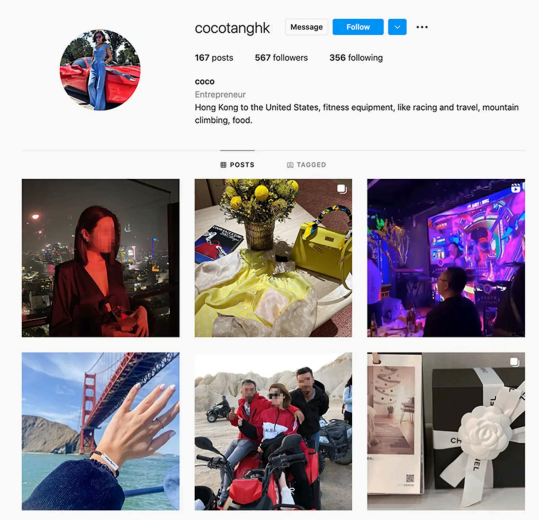
"Pig butchering," as the technique is known — the phrase alludes to the practice of fattening a hog before slaughter — originated in China, then went global during the pandemic. Today criminal syndicates target people around the world, often by forcing human trafficking victims in Southeast Asia to perpetrate the schemes against their will. ProPublica recently published an in-depth investigation of pig butchering, based on months of interviews with dozens of scam victims, former scam sweatshop workers, advocates, rescue workers, law enforcement and investigators, along with extensive documentary evidence including training manuals for scammers, chat transcripts between scammers and their targets and complaints filed with the Federal Trade Commission.

"We've had people from all walks of life that have been victimized in these cases and the paydays have been huge," said Andrew Frey, a financial investigator for the Secret Service, the federal agency that is taking a lead role in combating online crime and trying to help victims recover their stolen funds.

These swindles are not only highly organized but also systematized. Here's how the fraudsters typically go about it, including photographs, excerpts from text exchanges between scammers and targets, advice from training guides for fraudsters and police reports from pig butchering cases:

1. Create a fake identity

Pig butchers most often begin by creating a phony online persona, typically accompanied by an alluring photo (which itself might have been stolen) and images that convey a glamorous lifestyle.



This Instagram profile was reported to the Federal Trade Commission by a Florida resident who complained of losing $89,000 to a pig butchering scam. (Meta, which owns Instagram, said it's investigating the account, whose owner didn't respond to a request for comment.) Screenshot blurred by ProPublica

2. Initiate contact

Once they've got an online profile, fraudsters begin sending messages to people on dating or social networking sites. Alternatively, they may use WhatsApp or another messaging service and pretend to have stumbled on a "wrong number" as they contact you. (A spokesperson for Meta, which owns WhatsApp, previously told ProPublica that the company is investing "significant resources" into keeping pig-butchering scammers off its platforms.)

In December 2020, a Connecticut man received these messages on WhatsApp from a seemingly friendly stranger. He responded and eventually ended up getting tricked into two scams that cost him a total of $180,000.

[12/28/20, 12:06 AM] SCAMMER J: Long time no see, how are you recently

[12/28/20, 10:10 AM] SCAMMER J: 🙈 Are you not Kevin? Sorry, I guess I added the wrong person, sorry

[12/28/20, 10:16 AM] TARGET C: Not Kevin.

[12/28/20, 10:16 AM] SCAMMER J: Sorry, I made the wrong call. Since I have many business partners, my assistant saved the wrong number, please forgive me

[12/28/20, 10:17 AM] TARGET C: No prob. What country are you calling from?

[12/28/20, 10:17 AM] SCAMMER J: I come from Hong Kong. Hong Kong is a metropolis with technology, finance and food. Have you ever been here

[12/28/20, 10:18 AM] SCAMMER J: Acquaintance is fate, where are you from

[12/28/20, 10:18 AM] TARGET C: I'm from NYC originally

[12/28/20, 10:19 AM] SCAMMER J: Your place is a very beautiful place, I went there years ago

3. Win the trust of the target

The next step is starting a conversation with a potential victim to gain their trust. The scammers often initiate benign chats about life, family and work with an eye toward mining their targets for information about their lives that they can later use to manipulate them. They'll fabricate details about their own life that make them seem similar to you. After all, people like people who are like them.

When a Houston woman revealed that her brother was born with cerebral palsy, a crook countered with a similar-sounding tale:

[2/25/21, 6:32:38 PM] TARGET P: I have one brother that is handicapped and lives with my parents. Of course he's coming with them for the weekend

[2/25/21, 6:35:36 PM] SCAMMER C: I see. My parents are taking care of my brother. I hope he will live well

...

[2/25/21, 6:38:49 PM] TARGET P: My brother was born with cerebral palsy

[2/25/21, 6:39:19 PM] SCAMMER C: Sorry things, but also hard for your parents

[2/25/21, 6:39:29 PM] TARGET P: He's healthy over all but you have to do everything for him. He can't talk, dress, or feed himself

4. Sign them up

Before long, the swindlers will pivot to a discussion of investing. They'll make claims about their own purported investing successes, perhaps sharing screenshots of a brokerage account with gaudy numbers in it. They'll try to convince targets to open an account at their online brokerage. Unbeknownst to the target,

the brokerage is a sham, and any money deposited will go straight to the scammer. Most victims don't figure out that last part until it's too late.

Guides for scammers recommend touting the reliability of MetaTrader, a trading app that fraudsters use for nefarious purposes, by pointing out that the app is available in Apple's App Store, so it must be safe. (MetaTrader did not respond to requests for comment. An Apple spokesperson said the company has shared complaints with MetaTrader's parent company, and asserted that the parent has taken steps to respond to the complaints.)

5. Get them to put real money into the fake account

Once marks agree to learn investing tricks, the scammers will "help" them with the investment process. The fraudsters will explain how to wire money from their bank account to a crypto wallet and eventually to the fake brokerage. Typically the fraudster will ease the process by recommending a modest initial investment — which will inevitably show a gain.

A woman in Michigan became intrigued by her online boyfriend's references to making money trading gold and offered to become his student. Two days later, he was teaching her how to get started investing in a fake brokerage accessible through MetaTrader:

[3/16/21, 4:40:00 PM] TARGET T: What are you up to right now?

[3/16/21, 5:11:42 PM] SCAMMER L: I'm reading a book

[3/16/21, 5:14:39 PM] TARGET T: What book are you reading?

[3/16/21, 5:17:02 PM] SCAMMER L: A book about investing in gold

[3/16/21, 5:19:04 PM] TARGET T: Nice. You should teach me. Make me your student.

[3/16/21, 5:20:37 PM] SCAMMER L: 🥰 I don't want you to be my student. I want you to be my wife.🥰

6. "Prove" that it's legitimate

Scammers often allay initial doubts by letting targets withdraw money once or twice to convince them the process is trustworthy. For example, fraudsters allowed a Canadian man named Sajid Ikram to withdraw 33,000 Canadian dollars, according to a statement he filed with the Royal Canadian Mounted Police. That returned money helped convince him that his investment was real. He reported ultimately losing nearly $400,000, including money borrowed from several friends.

7. Manipulate them into investing more

That's only the beginning. Pig butchering guides offer insights on how to exploit marks' emotional and financial vulnerabilities to manipulate them into depositing more and more funds. It starts with assurances that the investments are risk-free, then escalates into pressure to take out loans, liquidate retirement savings, even mortgage a house.

Over a period of nine days, one scammer (who called herself Jessica) escalated her pressure, pushing the target, a California man, first to use his cash on hand, then to tap his retirement savings, then to borrow money.

[11/3/21, 8:03:13 PM] TARGET Y: I just don't want to risk

[11/3/21, 8:03:42 PM] SCAMMER J: When you need money, you can ask for it at any time

[11/3/21, 8:04:08 PM] SCAMMER J: This is not a risk, it is called maximizing profit

...

[11/8/21, 5:31:53 PM] TARGET Y: what can I do

[11/8/21, 5:32:27 PM] SCAMMER J: Your 401K can't move?

[11/8/21, 5:32:50 PM] TARGET Y: You know how that works. Heavy penalties plus double taxation

[11/8/21, 5:32:53 PM] SCAMMER J: Then you can earn it back with a fine.

...

[11/11/21, 6:20:05 PM] SCAMMER J: Borrowing money from the bank is not a big deal, I often do

[11/11/21, 6:22:11 PM] TARGET Y: I am not ignoring you. I am trying to think

[11/11/21, 6:22:45 PM] SCAMMER J: You are a wise man, this is borrowing a chicken to lay eggs

[11/11/21, 6:23:23 PM] SCAMMER J: Really rich people use bank money to invest

8. Cut them off

Once targets reach a limit and become unwilling to deposit more funds, their seeming investment success comes to a sudden stop. Withdrawals become impossible, or they suffer a big "loss" that wipes out their entire investment.

The California man was aghast when he discovered $440,000 he'd deposited was gone. Ultimately, the swindler persuaded him to invest another $600,000, which also disappeared into the swindler's account.

[11/18/21, 11:59:16 AM] TARGET Y: I lost all my money

[11/18/21, 11:59:18 AM] SCAMMER J: If the principal is not enough, it cannot be supported to the profit point.

[11/18/21, 11:59:34 AM] SCAMMER J: Don't worry,

[11/18/21, 11:59:46 AM] TARGET Y: I am negative $480k

[11/18/21, 12:00:01 PM] SCAMMER J: Prepare the funds and earn them back.

[11/18/21, 12:00:12 PM] TARGET Y: I don't have any money or funds to prepare

[11/18/21, 12:00:20 PM] TARGET Y: That's all I have!!!!!!!!!!!

9. Use their desperation to your advantage

Scammers will then turn the screws of manipulation tighter by telling victims there's a potential solution: If they deposit more cash into the brokerage, they can regain what they lost. Sometimes, the claim is that the investment is successful — but there's a "tax problem" that requires paying additional funds equal to, say, 20% of their total account value. If the victim pays, the scammer will claim that new obstacles have arisen that require paying new fees.

No matter how much targets pay, it's never enough, as detailed in the FTC complaint excerpted below, which was filed by a pig butchering victim in Maryland. This person lost almost $1.4 million, in part because the person kept meeting scammers' demands to pay taxes and various fees to get their money back:

"Once the trading has ended, I applied to withdrawal my money and profit from the website. The broker asked me to pay a tax on the profit of 88,587.90 usd on 8162021, this amount was wired again through Bank of America into a foreign account in Hong Kong. Another request for me to pay security deposit on my profits which was 83,950.00 usd wired out to a different foreign account in Hong Kong once again. The broker asked for a bank and withdrawal processing fee of 27,983.34 usd again was wired out to a different foreign account in Hong Kong. The very last wire was for expediting the withdrawal and the platform asked for 55,966.60 usd wired out to Hong Kong. At this point I already had to much money in the platform so I kept giving in."

10. Taunt and depart

Once the targets are aware that they've been swindled, the fraudsters often insult or taunt them. They soon go silent, and the websites of their phony brokerages stop working. Then they relaunch a new website under a different URL and restart the process with other targets.

After nearly four months of chatting and $30,000 in losses for the Michigan victim, her scammer seemed to revel in unveiling the financial — and emotional — deception:

> [7/1/21, 3:25:31 PM] SCAMMER L: I'm a liar, too.
>
> [7/1/21, 3:25:42 PM] TARGET T: What do you mean you are a liar?
>
> [7/1/21, 3:25:58 PM] SCAMMER L: But I am very kind, I only cheated you out of 30K, thank you for 30K
>
> [7/1/21, 3:26:16 PM] TARGET T: Wow.
>
> [7/1/21, 3:26:55 PM] TARGET T: *You deleted this message.*
>
> [7/1/21, 3:27:23 PM] TARGET T: You don't really love me? We are not getting married?
>
> [7/1/21, 3:27:44 PM] SCAMMER L: Surprise or surprise. I'm not surprised.

What to Do If You've Been Scammed

If you've been victimized, report the crime to your bank and law enforcement — the FBI, the Secret Service and local police — as quickly as possible. The longer you wait, the harder it is for your bank to reverse any fraudulent transactions and for law enforcement to trace, freeze or seize stolen funds. "We are definitely going to be more successful if you immediately report," said Erin West, deputy district attorney at the Santa Clara County District Attorney's office, which has had some success seizing assets linked to pig butchering scams.

Cezary Podkul
Cezary Podkul is a reporter for ProPublica who writes about finance.
cezary.podkul@propublica.org @Cezary

United States Secret Service Cybercrime Investigations

Exhibit 1-B

Cryptocurrency Investment Scams

The U.S. Secret Service continues to observe a significant increase in cryptocurrency and digital asset investment scams. These scams often target victims who use social media, online dating, or professional networking platforms.

The execution of these scams varies but typically involves a potential victim receiving a message from another registered user of these platforms. The message directs the potential victim to visit a website or to download a smartphone application supposedly associated with a cryptocurrency or digital asset investment opportunity. In some situations, the victim may also be enticed to make payments directly to the scammer in order for the latter to "manage" the investment in question. In reality, these alleged investment projects are scams designed to steal funds from the victim.

PIG BUTCHERING

One variation of these scams is known as "Pig Butchering" and occurs primarily on professional networking websites, through seemingly misdirected text messages, or online dating platforms. This begins with a message from a perceived professional contact, an individual sending a text in error, or an individual seeking a romantic relationship. The communication evolves into victims being convinced to make investments in cryptocurrency or digital asset projects. The victims make payments via traditional bank or wire transfers, bitcoin ATMs, or cryptocurrency transactions through smartphone applications or websites.

The victims in this situation are referred to as "pigs" by the scammers, because they use elaborate storylines to "fatten up" victims into believing they are in trusted partnerships. The scammers then refer to "butchering" or "slaughtering" the victims, after victim assets are stolen and ultimately causing victims financial and emotion ruin.

To learn more about digital assets, click here to visit the Secret Service Digital Assets page.

WARNING SIGNS:

- Receiving a solicitation on online dating, social media, or professional networking websites to invest in cryptocurrency or digital asset projects by either transferring funds directly to the individual or creating an account on a website or smartphone application.
- Receiving a request from a new contact to transfer funds via a Bitcoin ATM, bank or money remitting service, or smartphone application or website as an investment opportunity or to assist with a financial hardship.
- Receiving a communication promoting an online investment opportunity through a website which includes poor spelling or grammatical structure, dubious customer testimonials, or general amateurish web layouts.
- Receiving a request to create an account and share the account login credentials to assist with investment management.
- Receiving a message requesting to remotely connect to a computer and assist with creating an online account.
- Receiving a request to download software, plugins, or browser add-ons to use the processing power of a computer or smartphone for cryptocurrency mining or digital asset investment purposes.
- Receiving a request to pay taxes or fees to access the investment portfolio or release funds.

Exhibit 1-C

FEDERAL BUREAU of INVESTIGATION

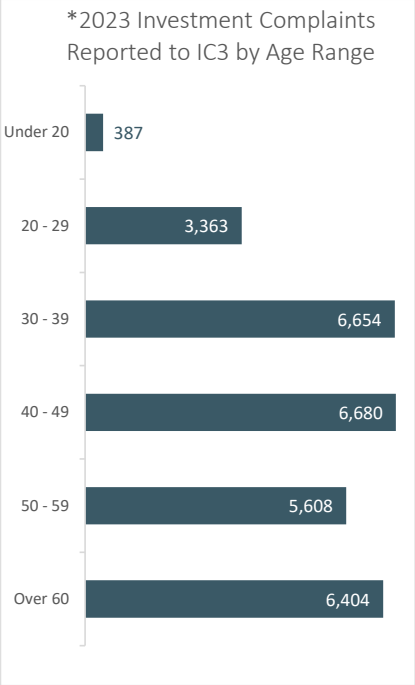
Internet Crime Report

2023

INTERNET CRIME COMPLAINT CENTER

INVESTMENT

In 2023, the losses reported due to Investment scams became the most of any crime type tracked by the IC3. Investment fraud losses rose from $3.31 billion in 2022 to $4.57 billion in 2023, a 38% increase. Within these numbers, investment fraud with a reference to cryptocurrency rose from $2.57 billion in 2022 to $3.96 billion in 2023, an increase of 53%. These scams are designed to entice those targeted with the promise of lucrative returns on their investments. [7],[8]



**Does not include complainants that did not provide an age range.*

IC3 publications in 2023 Related to Investment Fraud

- The FBI Warns of a Spike in Cryptocurrency Investment Schemes
- FBI Guidance for Cryptocurrency Scam Victims
- Increase in Companies Falsely Claiming an Ability to Recover Funds Lost in Cryptocurrency Investment Scams
- Criminals Pose as Non-Fungible Token (NFT) Developers to Target Internet Users with an Interest in NFT Acquisition

[7] Accessibility description: 2023 Investment Complaints Reported to IC3 by Age Range.
[8] Accessibility description: Chart shows Investment Fraud Losses Reported to the IC3 by Year for 2019 to 2023.

Exhibit 1-D

How Do Crypto Flows Finance Slavery? The Economics of Pig Butchering*

John M. Griffin† Kevin Mei‡

February 29, 2024

Abstract

Through blockchain addresses used by "pig butchering" victims, we trace crypto flows and uncover methods commonly used by scammers to obfuscate their activities, including multiple transactions, swapping between cryptocurrencies through DeFi smart contracts, and bridging across blockchains. The perpetrators interact freely with major crypto exchanges, sending over 104,000 small potential inducement payments to build trust with victims. Funds exit the crypto network in large quantities, mostly in Tether, through less transparent but large exchanges—Binance, Huobi, and OKX. These criminal enterprises pay approximately 87 basis points in transaction fees and appear to have recently moved at least $75.3 billion into suspicious exchange deposit accounts, including $15.2 billion from exchanges commonly used by U.S. investors. Our findings highlight how the "reputable" crypto industry provides the common gateways and exit points for massive amounts of criminal capital flows. We hope these findings will help shed light on and ultimately stop these heinous crimes.

*This paper is dedicated to all pig butchering victims, those defrauded and those enslaved, and especially the victim who gave us the impetus to write this paper. We are thankful for helpful comments from David Dicks, Gleb Domnenko, Cesare Fracassi, Sophia Hu, Brandon Kirst, Samuel Kruger, Alex Pettyjohn, Alex Priest, Marius Ring, Amin Shams, Michael Sockin, Qinxi Wu, and seminar participants at Baylor University, Integra FEC, the University of Rochester, the University of Texas-Austin and the University of Texas-Dallas. We thank Juan Antonio Artero Calvo, other research assistants, and especially Joseph Newcomer for excellent programming assistance. We thank Jan Santiago, Raymond Hantho, Chainbrium, and the United States Institute of Peace (USIP) for providing addresses collected as part of a USIP whitepaper. We further thank Integra FEC for use of their bulk tracing tools and for substantial crypto-research support. Griffin is an owner of Integra FEC and Integra Research Group, which engage in financial consulting, research, and recovery on a variety of issues related to the investigation of financial fraud.

†McCombs School of Business, University of Texas at Austin.

‡McCombs School of Business, University of Texas at Austin.

Crypto friendship or romance scams have proliferated. Random social media or text messages attempting to develop an online relationship are now commonplace. In a subset of cases, the friendly relationships slowly morph into full-blown scams known as "pig butchering" or *sha zhu pan*, which, in the extreme, bleed lonely, sick, and distressed victims, often with little exposure to investments and crypto, into the loss of their life savings. Though varied in nature, the origin of these scams is often even darker, as the manpower powering the communications is often enslaved in compounds thought to hold 220,000 victims in Southeast Asia.[1] This paper examines how these criminal organizations are financed through cryptocurrencies. How do criminal networks use crypto to move victim funds? Where does capital enter the network? Where do the funds exit? What obfuscation methods are employed? How pervasive is this activity? How can it be stopped?

Money flows are the lifeblood of organized crime by financing both current and future illegal activity. If illicit financial flows continue to grow and are uninterrupted, then the criminal network will typically expand. With this in mind, the international financial system has developed a framework, including Know Your Customer (KYC) and Anti-Money Laundering (AML) provisions, to combat the financing of transnational organized crime. However, with the emergence of Bitcoin and other cryptocurrencies specifically designed to create an anonymous alternative financial system, criminal networks now have new avenues to avoid detection and seizure of funds. Nevertheless, crypto is rarely used as a medium of exchange to purchase goods and services, and thus typically needs to be converted from and back to fiat currencies, such as U.S. dollars. The entry and exit points into the crypto ecosystem are typically crypto exchanges, which also purport to conform to international laws designed to mitigate illicit financial flows.

Although cryptocurrencies are designed to be anonymous, the nature in which the transactions clear on the blockchain provides a ledger that tracks the movement of funds. Thus,

[1]Section 1 provides a brief overview of the nature of the schemes and summary evidence compiled from government reports, investigative reporting, and documentaries.

the transactions are quasi-anonymous in that, by applying algorithms and substantial effort, it is often possible to determine where funds enter, move through, are swapped into different cryptocurrencies, and exit the crypto ecosystem.

We utilize data from pig butchering victim reports to determine the cryptocurrency addresses where victims were directed to send their funds by scammers. We start with 3,256 Ethereum addresses, 770 Bitcoin addresses, and 702 Tron addresses. Most addresses are used ten or more times, and 28% of addresses are used more than one hundred times. Of these initial sets, Ethereum addresses receive $5.8 billion in funds, compared to $389 million for Tron and $373 million for Bitcoin. Given that the Ethereum addresses represent approximately 88% of the total funds, we begin by examining Ether (ETH, the native cryptocurrency on Ethereum) and token (commonly known as ERC-20 tokens) transactions on the Ethereum blockchain.

Our primary approach is to track the flows entering and exiting scammer addresses and apply detailed bulk tracing algorithms to follow the paths of ETH and ERC-20 tokens that trade on the Ethereum blockchain. Based on blockchain information from an unfortunate U.S. victim who lost their retirement and life savings of approximately $465,000, we first show how their funds left their exchange's wallet in the form of ETH, USDC, and Bitcoin, were forwarded to another address, and subsequently swapped to other tokens using a relatively obscure decentralized exchange called Tokenlon. The pattern of this victim's funds is strikingly similar to that of many other adjacent nodes connected to the scamming network and many other reported victim cases.

We trace victim funds in bulk and follow their paths to centralized exchange deposit addresses from January 2020 to February 2024.[2] Figure 1 plots the resulting network for a three percent sample of nodes from the traced network and highlights many features. First, the figure shows how crypto often originates from large exchanges where investors commonly

[2]The data and analyses in this paper were last updated on February 20, 2024.

have accounts (Coinbase, Crypto.com, and Binance) and flows into the network. Second, funds are often swapped for Tether (known as USDT) through Tokenlon. Third, after circulating through various hops in the network, crypto exits the system through centralized exchange deposit addresses. Fourth, transactions in amounts above $100,000 and in particular $1 million commonly transfer funds to deposit addresses on Binance, Huobi, and OKX.

Across all exchanges, the scammer network initiated 104,460 deposits to centralized exchanges for amounts below $10,000, most commonly in small amounts clustering at round numbers, such as $100, $200 or $500. The transaction patterns mirror the characteristics of *inducement payments* in pig butchering scams, which are small payments from scammers to victims used to build trust. Of these, 31,980 transactions are sent to Western exchange deposit addresses, including Coinbase (15,249) and Crypto.com (15,433), while the remainder is concentrated in Binance, Huobi, and OKX.[3] We find 83% of potential inducement payments are sent from addresses used in more than ten transactions, suggesting limited monitoring by crypto exchanges.

Since scammers are unlikely to return large sums of stolen funds, we consider deposit addresses that receive more than $100,000 as more likely to be scammer deposit addresses. These addresses are rarely associated with Western exchanges, but are common within Binance, Huobi, and OKX, as well as exchanges such as Kucoin, Bitkub, and MXC. The common feature of these exchanges is that they have loose KYC procedures and are perceived to be outside of U.S. jurisdiction.[4] To more fully understand the scope of the network, we apply "deposit address clustering" (Victor, 2020) by tracking addresses that send funds into these deposit addresses and finding other recipient deposit addresses associated with the same user.[5] To avoid capturing payments made by criminals for things like inducement

[3]Throughout this paper, we include Coinbase, Crypto.com, Kraken, Gemini, and FTX as Western exchanges because these can be accessed by US-based users.

[4]Most notably, the DOJ announced on November 21, 2023 that Binance plead guilty to disregarding anti-money laundering laws, had the CEO step down, and agreed to pay a more than $4 billion penalty.

[5]This heuristic relies on the facts that an exchange customer may have multiple deposit addresses and

payments, we exclude all connections below $100,000 and only consider direct connections. Using this method to link additional deposit accounts likely controlled by scammers, we find $75.3 billion of Ethereum-based inflow through February 2024 to these addresses. Portions of this total could capture funds associated with other related networks that interact with the criminal networks; however, additional robustness analyses indicate that this is likely a conservative lower-bound estimate and the total size may be considerably larger.

After analyzing the network unveiled from tracing scammed funds forward, we also trace backwards from deposit addresses to find the largest sources of fund flows. We then collect the set of all nodes in the forward trace and backward trace and find $15.2 billion of funds that originate from five Western exchanges over the last four years, from over 1.25 million transactions from potential victims, averaging over $12,000 per transaction. Because our tracing is overly conservative to avoid potential false trace paths, this likely understates the scope of funds originating from Western crypto exchanges.

Within the trace path, we observe many distinct features of the network graph that shed light on how romance scams and money launderers operate. Scammers extensively recirculate and swap funds across different addresses and cryptocurrencies. These transactions incur costs, but may help obfuscate the true source of their funds. We estimate that transaction costs for a network of this scale total to 87 basis points as a portion of outflows to exchange deposit addresses. In contrast, Soudijn and Reuter (2016) find costs of 7-16% to move physical Euro bills from Europe to Columbia and money laundering commission estimates range from 4-12% (US Treasury Department, 2002) and 10-20% (US Treasury Department, 2007). Cryptocurrencies thus appear to be a much more cost-effective channel for moving illicit funds across borders. In total, scammer swap transactions may constitute more than 58% of Tokenlon transactions since 2022. We observe large inflows from potentially Chinese

any funds sent to these may only be accessed through the exchange; therefore, if a given blockchain address transfers tokens to two exchange deposit addresses, then it is likely that the two addresses are controlled by the same user. Deposit addresses are each assigned to a single verified account or user and thus provide an opportunity to examine the broader scope of the flows a user receives.

victims in 2020; however, after the Chinese financial authorities banned cryptocurrency trading in late 2021, there appears to be a dramatic decrease in Chinese victims and a shift to US-based victims. Overall, in the set of addresses touched by the criminals, we find $1.172 trillion dollars of volume, 84% of which is in Tether.

As a placebo test, we compare a trace analysis of pig butchering addresses to phishing scam addresses. Pig butchering networks have larger transactions and receive more funds than phishing scams. Transactions in phishing scams use proportionally more ETH and lead towards Uniswap, Kucoin, and Binance. This also highlights how our methods can be applied to other criminal crypto spaces. We also trace 770 Bitcoin addresses and find that the Bitcoin scam network funnels scammed funds into Tokenlon, Binance, Huobi and OKX. We follow these paths from the Bitcoin to the Ethereum blockchain and find 78% of Bitcoin cross-chain paths intersect with our Ethereum trace paths, further indicating the importance of the Ethereum network in criminal activity. We find the network of scammer nodes is highly connected, likely indicating that there exist widely-used services that funnel funds for extremely large and possibly related criminal networks.

It is our hope that this research, along with those of other researchers and practitioners will expose how crypto finances these dark activities.[6] This project highlights how large-scale tracing of tainted funds can help expose and understand criminal financial activity that can hopefully be used as a roadmap in other criminal contexts.

There are several other practical implications of our study. First, organized or "legitimate" crypto exchanges serve as the on- and off-ramps for billions of dollars in criminal proceeds. Users with a crypto exchange account should realize that crypto exchange users

[6] "One of the most effective ways to deter criminals and to stem the harms that flow from their actions–including harm to American citizens and our financial systems–is to follow the criminals' money, expose their activity, and prevent their networks from benefiting from the enormous power of our economy and financial system." From M. Kendall Day while acting Deputy Assistant Attorney General for the Criminal Division of the U.S. Department of Justice. He is now an attorney at Gibson Dunn and has previously served as counsel for Binance. He also states: "More broadly, money laundering undermines the rule of law and our democracy because it supports and rewards corruption and organized crime, allowing it to grow and fester" (U.S. Senate, 2018).

are frequent targets of scams, and their funds are just a quick transfer away from being irreversibly lost—a risk that is far less prevalent for traditional investment accounts. Second, our findings indicate that the large players in the crypto space are likely not sufficiently protecting their customers from scams. Third, the Ethereum network appears to drastically reduce barriers for illicit financial flows of transnational organized crime. Fourth, romance scammers prefer the stablecoin Tether over other cryptocurrencies and the Ethereum network over Bitcoin. Fifth, decentralized exchanges also serve as large swapping points to exchange crypto and obfuscate funds. Crypto hedge funds and users (many based in the U.S. and Europe) who might purport to engage in "arbitrage" or "liquidity trading" (PWC, 2023) may simply be making profits by facilitating low-cost money laundering. Finally, the large centralized crypto exchanges located in jurisdictions with opaque regulatory environments (Binance, Huobi, OKX, and others) seem to be preferential potential exit points that can further finance extremely large amounts of criminal activities. Such activity has continued as of February 16, 2024, despite recent crackdowns.

1 Related Literature and Background on Pig Butchering and Crypto

1.1 Related Literature

Our paper relates to three main literatures. First, there is a growing literature examining dark market activity in the crypto space. Meiklejohn et al. (2013) show how clustering algorithms can be used to identify Bitcoin transactions moving funds through the Silk Road, a darknet marketplace that operated between 2011 and 2013. Foley et al. (2019) find that 46% of non-exchange-related Bitcoin activity from January 3, 2009 to April 2017 is associated with darknet websites. They estimate that 27 million Bitcoin users conduct $76 billion in annual activity, which by some estimates is $3/4^{\text{th}}$ of the size of the U.S. drug trade. However, Makarov and Schoar (2021) use more conservative assumptions that account for potential double-counting and find that illegal activity, scams, and gambling account for less than 3% of Bitcoin volume over a more recent period from 2015 to 2021. In 2020, they estimated over $5 billion in dark market activities, online gambling, association with bitcoin mixers, and

scams. Cong et al. (2023b) examine 21,650 addresses involved in sextortion, blackmail scams, and ransomware. Though ransomware is underreported, they show that 43 ransomware gangs carried out 2,690 attacks from May 2019 to July 2021.[7] Amiran et al. (2022) studies the role of cryptocurrencies in terrorism financing. The academic literature mainly focuses on dark market activity in Bitcoin. In contrast, we detail the nature of activity on Ethereum, which includes techniques such as swaps between tokens and multiple transactions to seemingly evade detection. Since we only focus on funds in the network for one type of scheme and the funds we track are larger than those tied to the dark markets for Bitcoin in 2020 (Makarov and Schoar, 2021), the amount of criminal activity on Ethereum may be many times larger than previously estimated. We also make a methodological contribution by showing how bulk tracing multiple streams of funds moving through the network, including from Bitcoin to Ethereum, can help provide a more complete map of broader cryptocurrency networks.

Second, there is a growing literature related to other types of nefarious trading activity in crypto, including price manipulation, pump-and-dump schemes, and wash trading.[8] Cong et al. (2023a) examine common crypto scams including those of investment, ICO, rug pulls, phishing, blackmail, and Ponzi schemes. Gandal et al. (2018) show price manipulation of Bitcoin in 2014. Griffin and Shams (2020) show that Bitcoin prices were manipulated upward through the partially unbacked printing of Tether, which helped to fuel Bitcoin and other cryptos in 2017 and 2018. Li et al. (2018) and Hamrick et al. (2021) provide detailed evidence of pump-and-dumps of crypto tokens. Phua et al. (2022) estimate that 38.7% or $12 billion of capital from 5,935 ICOs were likely scams. Pennec et al. (2021) and Cong et al. (2023b) study crypto wash trading. Cong et al. (2023b) shows that wash trading accounts for trillions

[7] Chainalysis (2023) produces an annual summary report that tracks possible amounts of stolen funds, scams, sanctions, dark markets, ransomware, cyber security, fraud shows, child abuse materials, terrorism finance, and malware. They estimate over $20 billion in such total illegal activity in 2022 with $5.9 billion in scams in 2022, most of which they estimate to be investment and giveaway scams, not romance scams. They note that their figures are undercounting and that romance scams appear to be growing. Reiter and Bitrace (2024) examines blockchain addresses associated with two U.S. and two Chinese pig butchering victims and shows overlap in the addresses where funds are sent. Sokolov (2021) finds that Bitcoin transaction activity and fees increased around times of ransomware activity in 2014-2015.

[8] Griffin and Kruger (2024) briefly survey forensic crypto research.

of dollars of fake trading and over 70% of centralized exchange volume, with varying degrees across exchanges.

Third, we contribute to the literature on organized crime. In a survey of the literature, Levi (2015) notes that the lack of access to capital, and little overlap between the licit and illicit economy makes criminal enterprises rely on the re-investment of profits for growth. El Siwi (2018) notes that the recognition that "money is the lifeblood of organized crime" led to the adoption of the anti-money laundering (AML) regime in Italy.[9] Conrad and Meyer (1958) show how the strong economic incentives of slavery meant that the activity would have likely persisted if not for political intervention. Organized crime often purchase legitimate enterprises for money laundering (Mirenda et al., 2022) or utilize cash and various shell companies to obfuscate transactions moving into the banking system. Overall, examining criminal fund flows in the traditional banking system or through cash transfers is primarily limited to prosecuted case records, which explains the lack of academic research and reliable estimates of such activity. In a survey of the literature, Levi (2015) states: "we have little information about the mechanisms of financing." This paper seeks to partially fill this void.

1.2 Background on Pig Butchering

Romance and related friendship scams appear in various forms. In this section, we describe common variants discussed by documentaries, investigative reporting, and online blogs.[10] Romance scams often begin with seemingly random messages in the form of a text, WhatsApp message, or messages on social media platforms to the wrong person.[11] The scammers are looking for a victim who is lonely, going through tough times (such as

[9] Draca and Machin (2015) survey a growing literature on the economic relation between crime and unemployment, earnings, and education, and find that the economic incentives for crime are important. Leukfeldt et al. (2019) examine criminal investigations of organized crime in the Netherlands and find that technological knowledge for cybercrime is often gained through a smaller set of technically skilled enablers in online market places.

[10] In-depth descriptions by investigative reporters and documentarians include sources such as ProPublica, the BBC (via YouTube), and Faux (2023).

[11] The UN (2023) notes that contact in the forms of "Boo, Facebook, Grindr, Hinge, Instagram, Lazada, Line, LinkedIn, Meet Me, Muslima, OkCupid, Omi, Shopee, Skout, Telegram, TikTok, Tinder, WeChat, WhatsApp, and Wink."

a medical condition or divorce), and has sufficient cash.[12] First, there is a friendship or trust-winning stage, often spanning multiple months, which can also include the illusion of romantic potential.

After the scammer has earned the victim's trust, the topic of investments will arise. Victims, often with little or no crypto exposure, will be encouraged to open an account at a legitimate, well-known crypto exchange that victims can verify, trust, and easily transfer funds to that account. Scammers will claim to have an edge at another seemingly professional platform and encourage victims to transfer crypto funds to a provided crypto address; however, this second platform is fake or spoofed, and the crypto address is actually owned by the scammer. On the fake platform, it will appear as if the victim has quickly generated significant returns. Often the person is encouraged to withdraw funds from the platform back to the original account at the legitimate crypto exchange to build trust. This is known as an inducement payment because it induces the victim to send more funds. Through this process, the scammer can capitalize on both cryptocurrencies' reputation as a viable new technology, as well as the infrastructure connecting the traditional financial system and the cryptocurrency ecosystem to easily onboard funds.

Upon feeling more certain that the investment opportunity is real, victims often make larger deposits. Some victims have drained their savings and investment accounts, borrowed up to their credit card limit, paid penalties to convert their retirement funds, borrowed from friends and family, or placed another mortgage on their home. In the final stage where a victim seeks to withdraw funds, they are often asked to pay "taxes" on the fictitious profits before the funds can be withdrawn.[13] Ultimately, the scam does not end until the victim cuts contact, or the scammer is sure that the victim is bled dry of funds. The scammers

[12] A survey by the Global Anti-Scam Organization of 550 victims showed that victims from all stages in life are susceptible. Victims typically range between 30 to 60 years old, are often well-educated, and include both men and women. https://www.globalantiscam.org/post/statistics-of-crypto-romance-pig-butchering-scam

[13] A survey of 550 victims as of 2022 found that 77% emptied their savings accounts and 33% were driven into debt by scammers. https://www.globalantiscam.org/post/statistics-of-crypto-romance-pig-butchering-scam

REUTERS

Exhibit 1-E

A REUTERS SPECIAL REPORT

Crypto scam: Inside the billion-dollar 'pig-butchering' industry

Fraudulent crypto investment schemes directed from Asia known as "pig butchering" have become a global billion-dollar industry. But little is known about those who benefit. Reuters traced at least $9 million linked to such scams to an account registered to a well-connected representative of a Chinese trade group in Thailand.

By POPPY MCPHERSON and TOM WILSON | Filed Nov. 23, 2023, 11:45 a.m. GMT

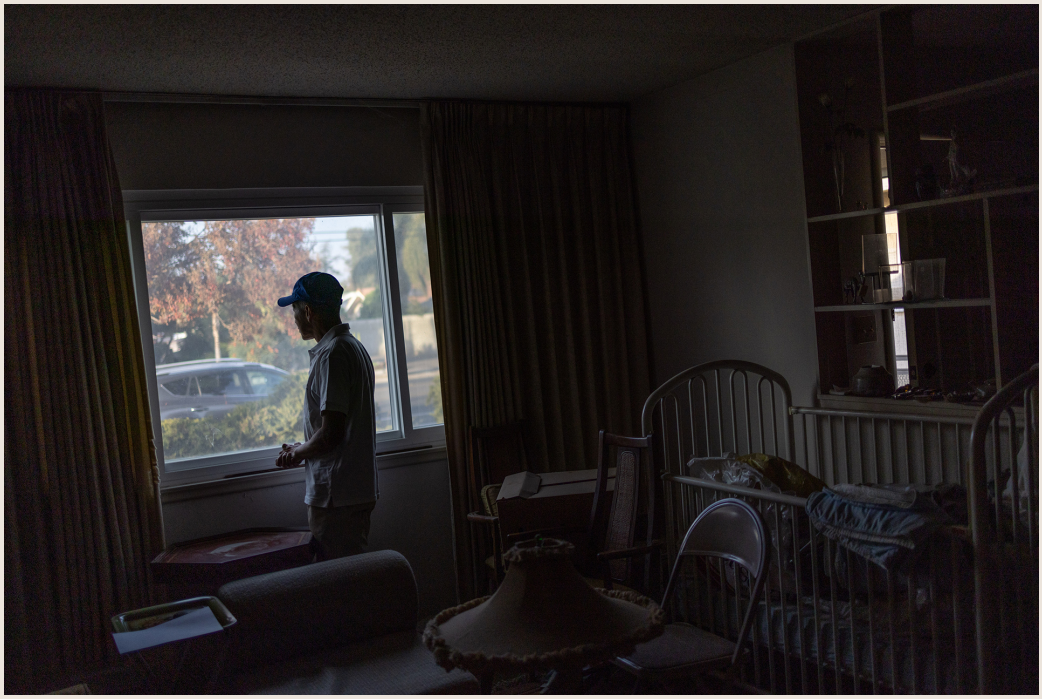
At a Thai police headquarters in October 2022, Chinese businessman Wang Yicheng congratulated one of Bangkok's most senior cybercrime investigators on his recent promotion, presenting the official with a large bouquet of flowers wrapped in red paper and a bow.

Wang, the vice president of a local Chinese trade group, wished the new cybercrime investigator "smooth work and new achievements," according to the group's website, which displays photographs of the event.

Over the past two years, Wang has forged relationships with members of Thailand's law-enforcement and political elite, the trade group's online posts show. During that time, a cryptocurrency account registered in Wang's name was receiving millions of dollars linked to a type of cryptocurrency investment scam known as pig butchering, a Reuters investigation has found.

In total, crypto worth more than $90 million flowed into the account between January 2021 and November 2022, according to registration documents and transaction logs reviewed by Reuters. Of that, at least $9.1 million came from a crypto wallet that U.S. blockchain analysis firm TRM Labs said was linked to pig-butchering scams. Two other major crypto-tracking firms also said the account received funds linked to such scams.

The victim of one of the scams was a 71-year-old California man. He sent money to crypto wallets that channeled more than $100,000 into the account in Wang's name, according to blockchain analysis company Coinfirm. The man's family told Reuters he lost about $2.7 million, his life savings, after falling prey to someone claiming to be an attractive young woman called Emma.



A 71-year-old man living in California says he lost about $2.7 million last year after falling prey to a crypto investment scam. Funds linked to that scam reached an account in the name of Chinese businessman Wang Yicheng, Reuters found. REUTERS/Carlos Barria

The previously unreported transactions provide rare insight into the finances of pig-butchering scams, which involve engaging unsuspecting people online. Scammers cultivate trust and then persuade victims to invest in fraudulent crypto schemes, sometimes via fake websites built to look like legitimate trading platforms. Sometimes the targets initially receive real returns to trick them into believing the scheme is legitimate.

Such scams have drawn intensifying scrutiny from global law enforcement over the past year, but little is publicly known about the people behind them.

Wang, who is 41 according to the account registration documents, didn't respond to detailed questions for this article. Neither did the Thai government, the Thai police or the Bangkok-based trade group Wang represented, the Thai-Asia Economic Exchange Trade Association.

Some aspects of the pig-butchering operation remain murky. Lisa Wolk, a blockchain intelligence analyst at TRM, said the crypto account in Wang's name "is a node in a money laundering network and not necessarily the ultimate recipient of funds." Reuters was unable to determine whether anyone else benefited from the account or used Wang's identity to open it.

Chinese businessman Wang Yicheng has forged relationships with some of Thailand's law-enforcement and political elite. Here, he congratulates a police cybercrime investigator on a promotion. The photo was posted by the Thai-Asia Economic Exchange Trade Association to its WeChat account in October 2022.

In January, agents from the U.S. Federal Bureau of Investigation and the U.S. Secret Service attended a briefing about cyber fraud, according to Erin West, a California prosecutor specializing in cybercrime who participated. A 72-page presentation prepared for the attendees, which Reuters reviewed, provides details on cyber scams operated from Southeast Asia and cites Wang as among alleged beneficiaries. The presentation depicts money flowing into a crypto wallet identified as belonging to Wang, notes his role at the Thai-Asia association, and includes a picture of his identity card and other photos of him.

The FBI and Secret Service declined to comment on the briefing, or on whether Wang was part of any investigation. The briefing was given by the Global Anti-Scam Organisation, a U.S. non-profit that advocates for fraud victims and investigates cases.

The crypto account registered to Wang was held at Binance, the world's largest crypto exchange, according to three blockchain analysis firms. Asked about the account, Binance spokesperson Jessica Jung declined to comment on individual users or Reuters' findings. In an August post on its website, the company said the number of reports of pig-butchering scams it had received this year was double that of 2022, an increase it attributed to an influx of inexperienced crypto investors and scammers looking to exploit them.

Crypto fraud has emerged as a multibillion-dollar criminal specialty that has entrapped victims around the world. In the United States alone, victims reported losses of $2.6 billion from pig butchering and other crypto fraud last year, more than double the previous year, according to the FBI. The true scale of the losses is unknown because victims are often too embarrassed to report crimes to authorities.

In April, the U.S. Department of Justice said it seized about $112 million worth of crypto linked to pig-butchering scams, without identifying suspects. A warrant that resulted in the seizure of more than half that amount specified a Binance account registered in Thailand.

Wang is vice president of a Bangkok-based trade group called the Thai-Asia Economic Exchange Trade Association. The screenshots of him here are from the association's website. REUTERS/Florence Lo

'Absolute devastation'

West, the California prosecutor, said many victims in the hundreds of pig-butchering cases she has handled since early 2022 have lost more than $1 million. Many are never able to recover their money. West said at least one victim died by suicide and another attempted suicide. "I've never seen this level of absolute devastation," she added.

Pig-butchering scams originated in China, financial crime specialists say. Many are now run by criminal organizations out of Southeast Asia that use victims of labor trafficking to contact individuals around the world, the U.S. Treasury said in September. Cases are difficult to prosecute. Perpetrators are typically "ruthless transnational organized crime syndicates" that thrive on corruption, Jeremy Douglas, regional representative of the United Nations Office on Drugs and Crime, told Reuters.

Erin West, a California-based prosecutor specializing in cybercrime, said many of the victims of pig-butchering scams she has dealt with have lost more than $1 million. Erin West/Handout via REUTERS

Several scams connected to deposits made into the account in Wang's name were run from an industrial park on the Myanmar-Thai border, one of the blockchain analysis firms told Reuters. Workers are trafficked to the area, known as KK Park, by gangs that force them to con people online, according to two former workers and groups that support workers or scam victims.

The Thai government, Myanmar's ruling military junta and the Myanmar border guard that controls the area didn't respond to questions about the industrial park or whether gangs operate there. Reuters was unable to contact the park's owners.

"They will try to use your weakness to gain what they need."

The 71-year-old crypto investment fraud victim, on the people who scammed him

China has announced a crackdown on cyber scams in recent months in partnership with Thailand and Myanmar. Thailand has also said it is combating cyber fraud. Thai police in September announced the arrest of several Chinese nationals in connection with a crypto investment fraud operation.

Binance publicly said it assisted Thai police with a probe into "a significant pig butchering scam," and that about $277 million of assets were confiscated. Thai police didn't respond to questions about the operation or whether there was any connection to Wang.

Birds' nests to crypto

Wang was born in 1982 in the port city of Ningbo on China's east coast, according to the identity card used to register the crypto account.

In his late twenties and thirties, he started several businesses in China, mostly related to technology, including computer and electronics sales, according to publicly available corporate records. The records show one business involved selling birds' nests, a culinary delicacy in China often used in soups.

By 2018, Wang had moved south to the coastal city of Xiamen, according to the identity card. By the following year, all of his Chinese-based businesses had been de-registered, apart from one in Ningbo that shut down in September of this year, the corporate records show. That firm, called Ningbo Laizheda E-Commerce Company, didn't respond to a request for comment.

RELATED CONTENT


How crypto giant Binance became a hub for hackers, fraudsters and drug traffickers


Binance's Zhao pleads guilty, steps down to settle US illicit finance probe


'Hundreds of thousands' trafficked into SE Asia scam centres - UN

Wang branched out into businesses in Thailand. In 2018, he became a partner of the Thai arm of a major Chinese maker of crypto production gear called Bitmain, according to Thai corporate records. In response to Reuters' questions, Bitmain said Wang was not an employee but a "close partner" and customer who purchased its bitcoin mining machines. Bitmain said it supplies "digital miners in the legal way."

$2.6bn

Reported losses from pig butchering and other crypto fraud last year in the U.S. alone.

The crypto account in Wang's name was registered in November 2020, according to the financial records Reuters reviewed. The three blockchain-analysis firms determined the account was with Binance. The documents, which relate to the Binance account, span two years to November 2022. They show that the account was accessed mostly from Bangkok.

Deposits started arriving in the account in early 2021 and quickly increased in size to include sums of more than $100,000, the financial records show.

By October 2021, Wang had become vice president of the Thai-Asia Economic Exchange Trade Association, according to the group's website. The group formed in 2019 to unite overseas Chinese businessmen in Thailand, the website says. It says the group is committed to promoting cultural exchanges and business investment between Thailand and China and other Asian countries.

The group also publicly espoused the Chinese government's political positions. In an undated video on the group's website, Wang and other association leaders chant, "Build a Thai-China bridge, tell China's story well!"

The Thai-Asia trade association until recently shared its small office building in Bangkok with another Chinese group, the Overseas Hongmen Cultural Exchange Center, corporate records and photographs show. The two groups also shared some common leadership: The head of the Overseas Hongmen group was an adviser to the Thai-Asia association, according to the Thai-Asia association website.

In February, Thai police said it raided the Hongmen group's part of the office, alleging the group had ties to the 14K Triad. The United States has called the 14K Triad one of China's largest criminal organizations. In 2020, Washington sanctioned Wan Kuok Koi, known as Broken Tooth, accusing him of being a 14K leader and attempting to create a network of businesses, including cryptocurrencies, to export crime and co-opt elites in Southeast Asia. He could not be reached for comment.

A month after the Thai police raid, the Overseas Hongmen Cultural Exchange Center was dissolved, corporate records show. Neither the Hongmen center nor the Thai-Asia association responded to questions on the raid.

The Thai-Asia Economic Exchange Trade Association, based in the suburbs of Bangkok, says it formed in 2019 to unite Chinese businessmen in Thailand. REUTERS/Staff

The association shares a building with another Chinese group called the Overseas Hongmen Cultural Exchange Center, which Thai police raided earlier this year. REUTERS/Staff

‘Honorary advisers’

Wang and other trade group leaders have courted senior officials in Thailand. The trade group’s website details at least 100 meetings since its formation with officials in the Thai police and government, as well as with staff of the Chinese embassy in Thailand and visiting Chinese officials.

Among the Thai-Asia Economic Exchange Trade Association’s “honorary advisers” is Kornchai Klaiklueng, assistant to Thailand’s national police chief and former head of the cybercrime police. Photo via Royal Thai Police website

Reuters found no evidence that Thai and Chinese officials were aware of the pig-butchering connections to the account in Wang's name. The Thai government, the Thai police and the Chinese embassy in Bangkok didn't respond to questions about the meetings. China's foreign ministry, in response to questions about Wang and his interactions with Chinese officials, said, "We are not aware of relevant circumstances."

The association also appointed at least eight senior Thai officials as "honorary advisers," according to its website. It says some of the trade group's leadership served as advisers to the police, including its president, who advised the police cybercrime unit. The association's representatives and officials frequently exchanged gifts, from whisky and fine wines to "precious Buddha statues," the website details.

Among the advisers named on the association's website is Kornchai Klaiklueng, who headed the Thai police's cybercrime division until last year and is now assistant to the national police chief. Photos posted on the trade group's social media account show Kornchai participated in events with Wang or other trade group leaders on more than 10 occasions between December 2019 and August 2023.

Another listed adviser is Chatchaphantakarn Klaiklueng, the head of the Bangkok division of the cybercrime police. Chatchaphantakarn is the police official to whom Wang paid his congratulatory visit in October 2022. Kornchai and Chatchaphantakarn are brothers according to Chatchaphantakarn's Facebook page. They have another brother, Ponganan Klaiklueng, who's also a cop, according to Ponganan's social media account and a local media report. Ponganan is also an adviser to the trade group, the association's website says.

During a November 2021 visit to the trade association's office, Chatchaphantakarn praised the friendship between Thailand and China and said his family has "Chinese blood," according to a video posted to his Facebook page. At the time, Chatchaphantakarn ran training for the Thai police, the trade association's website says.

Weeks later, the association announced on its website that it was funding a renovation of a police shooting range and other facilities. The association didn't respond to questions on the funding.

Wang and other members of the Thai-Asia trade association take part in a pistol shooting competition organized by the Thai military. The photo was posted by the Thai-Asia Economic Exchange Trade Association to its WeChat account in August 2022. Faces pixelated by Reuters.

The Thai police and the three brothers didn't respond to requests for comment on the police officials' relationship with Wang.

Among the most senior of Wang's contacts is Thammanat Prompao, Thailand's agriculture minister. A political power broker, he played a key negotiating role in the recent formation of Thailand's coalition government.

Thammanat was sentenced to prison in Australia on drug-trafficking charges in the 1990s, according to Australian and Thai court records. He served four years in prison and was released in 1997, according to Australian media reports. He told Thailand's parliament in 2020 that he was caught with flour.

In a December 2021 meeting with Thammanat at his office in Bangkok, Wang and other representatives of the trade group presented the politician with a hamper that included bottles of Johnnie Walker whisky, according to the association's website. Thammanat has also held an honorary position at the association, according to a video and articles on the trade group's website.

Thammanat didn't respond to requests for comment. In a video published in November 2022 by Thai PBS, a local TV channel, Thammanat denied any involvement with Chinese criminals in response to media reports alleging that he had such ties.

Thammanat Prompao, Thailand's agriculture minister, in 2019. He is also among the Thai officials that the Thai-Asia trade group says held an honorary position at the association. REUTERS/Soe Zeya Tun

'Complex layering scheme'

In 2022, the volume of crypto reaching the account in Wang's name mushroomed to almost $79 million, a near six-fold increase on the previous year, the account records seen by Reuters show.

Coinfirm, the blockchain analysis firm that reviewed the transaction records for Reuters, said deposits from funds linked to pig-butchering scams it previously investigated began entering the account as early as February 2022. Stolen crypto was moved to the account via a "complex layering scheme," involving multiple different wallets, Coinfirm's then-head of fraud investigations Roman Bieda told Reuters in May. The crypto moved between "dozens" of wallets and was mixed with funds from other sources, he said.

Some $9.1 million flowed to the account registered in Wang's name from the wallet linked by TRM to pig-butchering scams. The funds were moved in more than 50 transactions between August and October 2022.

Coinfirm linked the funds to pig-butchering scams based on information gathered from multiple victims and from publicly-available information, Bieda said.

Coinfirm said it identified funds originating from four pig-butchering scams. One involved a website called bigoneit.site, which channeled some of the funds the California man invested in the scam to the Wang-registered account. The site was a fake version of a legitimate crypto exchange called BigONE.

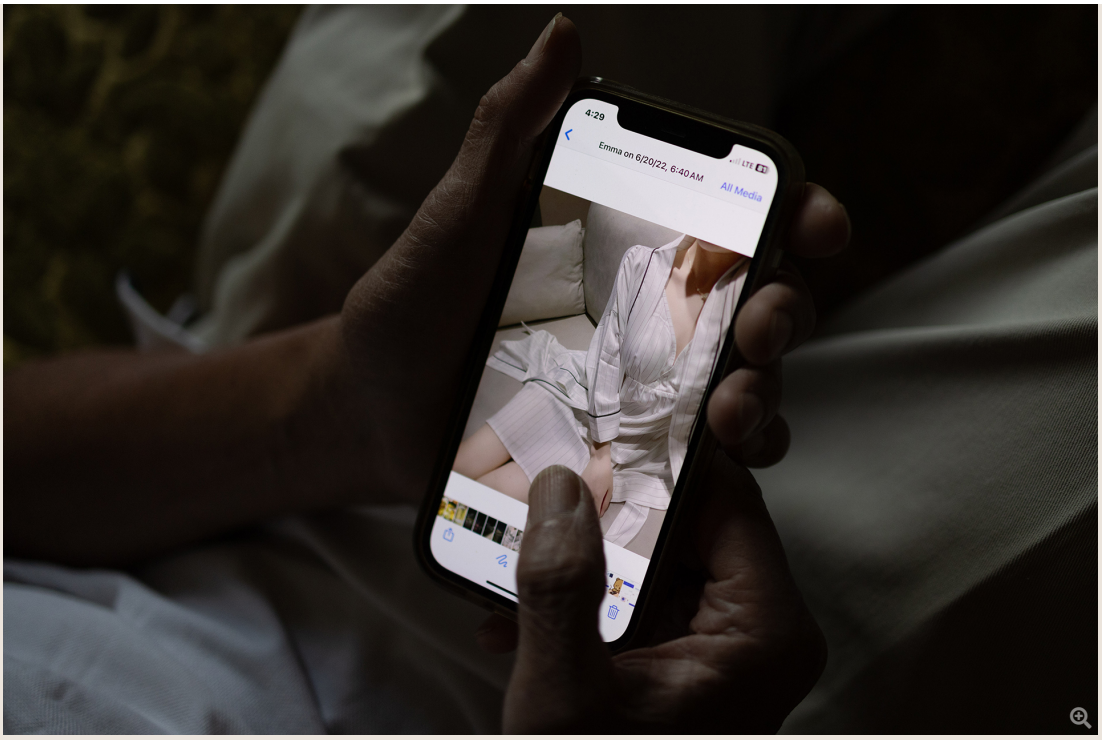
The 71-year-old man works in a home improvement store and lives alone. A Chinese American who immigrated to the United States in the 1980s, he built up his savings by working and contributing to a pension, while also trading stocks, according to his niece.

In March 2022, he received a text message from someone claiming to be a young woman, according to messages he shared. The texter later identified herself as “Emma.” Over the following weeks, the man and Emma built up a rapport. Emma encouraged him to send crypto to the fraudulent website, the messages show, interspersing small talk and trading tips with what she said were photos of herself - a slim young woman with long hair.

By July last year, the California man had poured some $2.7 million into the scam, his niece said. The victim, who spoke on condition of anonymity, said Emma’s “smooth talking” convinced him that he could make money. He discovered he’d been scammed when he was unable to withdraw his funds. His family reported the theft to law enforcement, incident reports show.

“I trusted her,” he said, adding, “my heart is too kind.” Scammers will “try to use your weakness to gain what they need.”

Someone claiming to be a young woman called Emma contacted the 71-year-old California man. The two built up a rapport, and she encouraged him to send crypto to a website purporting to be a digital currency exchange. REUTERS/Carlos Barria



"Emma" interspersed small talk and trading tips with photos, including this one, of a woman that she said was herself. REUTERS/Carlos Barria

The genuine crypto exchange BigONE said it takes fraudulent websites seriously, and that it had received at least 10 reports of such sites.

"We always emphasize in any promotional material that only big.one and bigone.com are official domains," the Seychelles-registered company said.

Reuters was unable to reach the operators of the fake website.

More than $102,000 originating from fraudsters' wallets that the California man identified were deposited into the account in Wang's name between June 26 and Oct. 23, 2022, according to Coinfirm.

Nearly all of the crypto deposited in the Wang-registered account was moved to other wallets, the transaction records reviewed by Reuters show. Between January 2021 and October 2022, about $87.5 million was transferred to almost 50 other crypto wallets, including at least five registered at regionally based crypto exchanges, Coinfirm said.

The account goes dark

On Nov. 3, 2022, activity in the crypto account registered to Wang abruptly stopped, the financial records show. The pattern of transfers to the account suggests Binance may have started an investigation and suspended the account, Coinfirm said.

Any financial firm should carry out additional checks on clients whose accounts process large amounts of money, said Ross Delston, a former U.S. banking regulator and expert witness on anti-money laundering issues. Red flags likely to trigger checks on the source of funds include a high volume of transactions and frequent deposits of round-numbered figures, Delston said.

The account registered to Wang frequently received such deposits, according to the financial records.

Wang, at far right, and other trade group representatives present Thammanat, center, with a hamper during a meeting in Bangkok. Other faces pixelated by Reuters. The photo was posted by the Thai-Asia Economic Trade Exchange Association on its WeChat account in December 2021.

Binance didn't respond to questions about the activity in the account in Wang's name or any checks it made on the account. Binance said that it works to combat pig butchering, helping law enforcement identify, freeze and seize criminal assets, providing investigative training, and running crime prevention campaigns.

Binance chief Changpeng Zhao stepped down and pleaded guilty to breaking U.S. anti-money laundering laws on Tuesday, as part of a $4.3 billion settlement resolving a years-long probe. Over five years, Binance processed transactions by users who "laundered proceeds" of criminal activity including scams, U.S. authorities said.

Wang has continued to court officials. In August, he helped host an event in Bangkok, according to photos and a description published on the Thai-Asia association's WeChat account.

Standing on a red carpet under a chandelier and flanked by floral decorations, Wang "warmly welcomed" the guests. They included a government minister, senior police officers and Chinese embassy officials, according to the trade group's post.

Among those in attendance: Kornchai Klaiklueng, the assistant to the national police chief who previously headed up the cybercrime unit.

The trade group Wang represents hosted an event this year attended by police officials Kornchai Klaiklueng, second from right, and Ponganan Klaiklueng, fourth from right. Other faces pixelated by Reuters. The photo was posted by the Thai-Asia Economic Exchange Trade Association to its WeChat account in August 2023

REUTERS INVESTIGATES

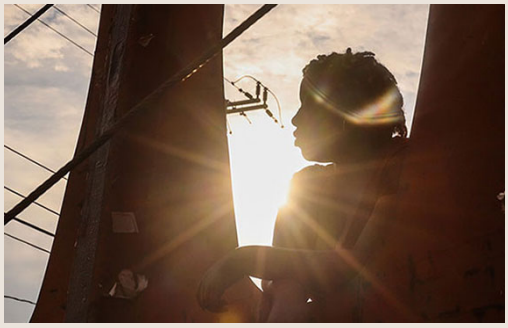
More Reuters investigations and long-form narratives

Got a confidential news tip? Reuters Investigates offers several ways to securely contact our reporters

Pig Butchering
By Poppy McPherson and Tom Wilson
Additional reporting by Chen Lin in Singapore, Carlos Barria in San Francisco, the Reuters Sydney bureau and the Reuters Beijing bureau
Photo editing: Edgar Su
Art direction and lead illustration: Eve Watling
Edited by Cassell Bryan-Low

Follow Reuters Investigates

OTHER REUTERS INVESTIGATIONS



OnlyFans Exposed

OnlyFans makes amateur porn creators rich. It has also faced 100-plus complaints of nonconsensual porn–including a woman who says her rape was filmed and sold.

Hanging Judges

Judges involved in Trump cases face an unprecedented wave of threats following the ex-president's attacks on judges as corrupt and biased.

Ethiopia's Quiet Crackdown

How a secretive Ethiopian security committee ordered extra-judicial killings and illegal detentions to crush an insurgency in the largest region, Oromiya.

Putin's war

Reuters traced one Russian officer class through training to the Ukraine battlefield, where some died and some were decorated.

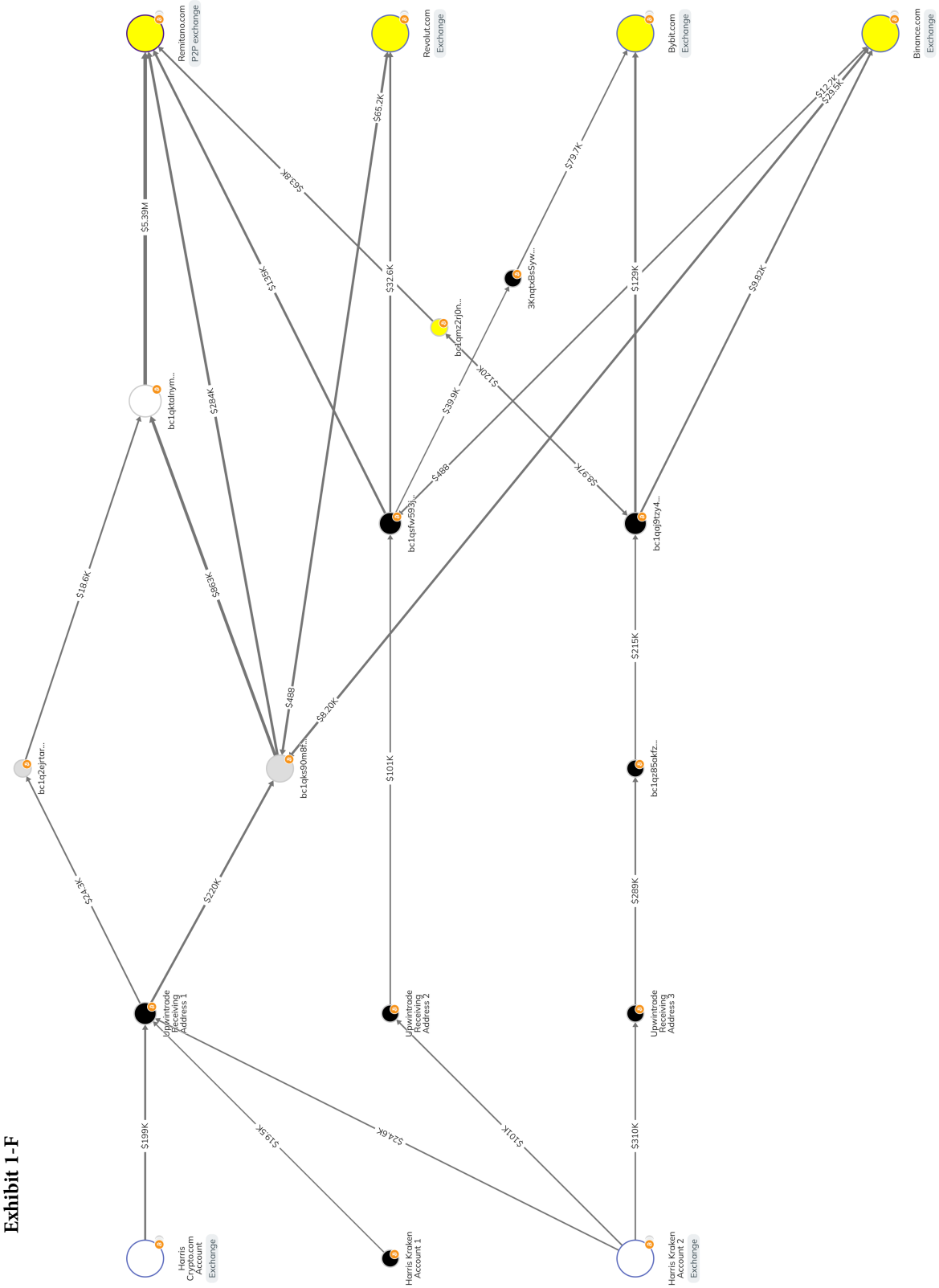

Remitano.com
P2P exchange
Revolut.com
Exchange
Bybit.com
Exchange
Binance.com
Exchange
$5.39M
$65.2K
$79.7K
$12.2K
$15.5K
$63.8K
$32.6K
$129K
$9.82K
$513K
$284K
$39.9K
$120K
$488
$89.7K
$18.6K
$963K
$488
$8.20K
$215K
$101K
$289K
$42.3K
$220K
$199K
$19.5K
$24.6K
$101K
$310K
bc1q2ejrtar...
bc1qktalnym...
bc1qs90m8l...
bc1qsfw593j...
bc1qqj9tzy4...
bc1qs85akfz...
3Knqtx8ssyw...
bc1qmz2rj0n...
Upwintrade
Receiving
Address 1
Upwintrade
Receiving
Address 2
Upwintrade
Receiving
Address 3
Harris
CryptoCom
Account
Exchange
Harris Kraken
Account 1
Harris Kraken
Account 2
Exchange

Exhibit 1-F

Exhibit 1-G

Receiving Exchange Transaction Ledger

This ledger collects all transactions in which assets traceable to the Harrises were transferred to addresses associated with one of the Receiving Exchanges.

Date	Receiving Exchange	Asset	Transaction Hash	Initiating Address	Receiving Address	BTC Amount	USD Amount
3/1/24 17:12	Revolut	BTC	7b9e47576406a7af8a3c54335e57fcb8fa6713c0269ce5a564b9e9b0cf75b146	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	bc1q7gku9m33re89mes97dwq4lawwxg3hj6g28umcy	0.09752991	5966.83893
3/6/24 14:41	Revolut	BTC	2bfd36d30659e28d3c865868c93656c6363a30d176651684d7dbb33f41bfe9ac	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	bc1q7gku9m33re89mes97dwq4lawwxg3hj6g28umcy	0.02977233	1992.77965
3/20/24 16:37	Revolut	BTC	ed6622240afe8d924af23a5caf35366b50846f4b3d847120319c7965e8e0daeb	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	bc1q7gku9m33re89mes97dwq4lawwxg3hj6g28umcy	0.05501777	3406.92149
3/31/24 8:13	Remitano	BTC	fb9762f35517d528af8ec68457955201798d827b61b2a86088a62c5e773a76ead	bc1qks90m8fsjdtck0euylpq0zt6p8u2j52wwqsy7t	38ZWvd5Be2PqMu5xcvy9PY3T4frKvniNyf	0.07144691	5022.91282
4/1/24 4:38	Remitano	BTC	a89ae6523e72509ed8d7c997bdb8f21500b3276f4c198dfe9b322a6fd52747a5	bc1qks90m8fsjdtck0euylpq0zt6p8u2j52wwqsy7t	38Ep5mFzh6oNbuFXSL1Hvk3g1TwXUMX8xv	0.00990962	699.2219
4/8/24 12:48	Remitano	BTC	cf7d232b637bd5d97625cb913611c1d55b23605925d3c2c71fa8e4b65bc6551f	bc1qks90m8fsjdtck0euylpq0zt6p8u2j52wwqsy7t	3M5RWiGdcEDRseLUqaG15HgPLL7bf3644A	0.01154274	800.57351
4/15/24 13:55	Remitano	BTC	ab3b200823c9069e753c57bf9b757cdbbfbde538c0c7493eaeb614b6754a8876	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	3M5RWiGdcEDRseLUqaG15HgPLL7bf3644A	0.00708734	468.80706
4/15/24 17:39	Remitano	BTC	9926d07a6497459676fc66f2157cfed354553e78c1cb657b90b9d1319073e8fe	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	38ZWvd5Be2PqMu5xcvy9PY3T4frKvniNyf	0.02150766	1387.46087
4/15/24 18:57	Remitano	BTC	f4be2147dfe0e1295361200b0b2be9d027233d73e4ba912c3708c86f9c95cd9	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	3M5RWiGdcEDRseLUqaG15HgPLL7bf3644A	0.03127239	1987.00951
4/16/24 11:13	Remitano	BTC	931acaae1300e658ea1e2ea719ff913a800fd54185e5c5d9cd0dfa0c178ce2db	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	38ZWvd5Be2PqMu5xcvy9PY3T4frKvniNyf	0.02948534	1870.76433
4/16/24 14:43	Remitano	BTC	be23f141eddc2a1c7d670583470b9bc7928b1e882c70be71ae9f1b5ba7874278	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	38ZWvd5Be2PqMu5xcvy9PY3T4frKvniNyf	0.08996085	5588.67567
4/16/24 16:41	Remitano	BTC	2619d35853ef76b7fb487c0e961226445668557395188c0ccb4a91ba2e830df8	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	3M5RWiGdcEDRseLUqaG15HgPLL7bf3644A	0.00634298	402.44476
4/17/24 11:43	Remitano	BTC	346183bbf072b4f7acac1692533a2a48f26f6488a9bb867c3ff4dede698faa8	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	38ZWvd5Be2PqMu5xcvy9PY3T4frKvniNyf	0.03391575	2139.667
4/17/24 18:17	Remitano	BTC	86f651035708c4ae93c7403d0c4b3e2bf03dd6ef2aa50083b02b43c971058466	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	3M5RWiGdcEDRseLUqaG15HgPLL7bf3644A	0.02025719	1230.67352
4/18/24 7:25	Remitano	BTC	79c61dce88e1ce29ff729ebbfb553b9533f3eb91b723e7dc30ef21aaf8bd790d	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	3M5RWiGdcEDRseLUqaG15HgPLL7bf3644A	0.00972095	593.12065
4/18/24 12:14	Remitano	BTC	2a6ff4adeecd0cbbda806533e340816d525ce5468200c1b744feac56ff4aa040	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	3M5RWiGdcEDRseLUqaG15HgPLL7bf3644A	0.02841014	1782.10018
4/18/24 16:32	Remitano	BTC	80854bf6d99a24945d3f92d8eb4c99b11ca9fc07bfb4b0f0cfc6de761ad1321d	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	3M5RWiGdcEDRseLUqaG15HgPLL7bf3644A	0.01390539	881.30318
4/19/24 6:26	Remitano	BTC	fc624623c1beab88154896dada59d8bffd2af05560cd15563493c1b93830b817	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	38ZWvd5Be2PqMu5xcvy9PY3T4frKvniNyf	0.03392351	2106.43931
4/19/24 13:12	Remitano	BTC	5726e3cbd6d5095602878 9e8f3bab4e9fb921246a95b5269962a1207e7a6bb33	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	38ZWvd5Be2PqMu5xcvy9PY3T4frKvniNyf	0.03503836	2289.11773
4/20/24 9:39	Remitano	BTC	840d03124b9624a3d7e82c01d8d5ebf7ee332434f494a8f8d4cdb3f6c68c4612	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	3M5RWiGdcEDRseLUqaG15HgPLL7bf3644A	0.00785066	501.24533
4/20/24 12:31	Remitano	BTC	ddaa23422a17720a646a02afe93b7a6245e93b6a9c22cb75b23668e9a62aadc8	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	3M5RWiGdcEDRseLUqaG15HgPLL7bf3644A	0.04490203	2866.91649
4/20/24 21:16	Remitano	BTC	79e19499bf7516bcadda58cc988073a7d7fac80420283bc1a65a5d8a161cb8ad	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	3A34Ggh1EUNXe4K8ayTLNLdKYAUDTnEU63	0.06175687	4003.38972
4/21/24 4:56	Remitano	BTC	ff20937d45a223781f29fc368faca6cdc3b0a70999ae7004fbe61926b032496b	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	38ZWvd5Be2PqMu5xcvy9PY3T4frKvniNyf	0.06246087	4053.32071
4/21/24 14:21	Remitano	BTC	b6126d8e83154587f02e1ff806947ab4bf16b4aea4e9ebb61be481441ae466c3	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	38ZWvd5Be2PqMu5xcvy9PY3T4frKvniNyf	0.03076209	1999.74349
4/22/24 10:41	Remitano	BTC	64898a49a4a8659b3932bc7b46ed20e6e065dab12e7c3da2ecdeff6e98ab00aa	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	3M5RWiGdcEDRseLUqaG15HgPLL7bf3644A	0.02159675	1402.83461
4/24/24 8:56	Remitano	BTC	e5baa00245d3520e400c3b35219fe05f965d15d69dc72f6ba716456d17b13fa	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	38ZWvd5Be2PqMu5xcvy9PY3T4frKvniNyf	0.00935874	623.65109
4/24/24 12:11	Remitano	BTC	6d7969f6eed2b0a5cb205a96330abfa544ffe69221b9a04281f67e106569b2ec	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	38ZWvd5Be2PqMu5xcvy9PY3T4frKvniNyf	0.04056038	2699.34561
4/24/24 21:44	Remitano	BTC	90bb3b020da0719965099ed81d937ab4677573655a61986c21f582bd9f1c4b637	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	38ZWvd5Be2PqMu5xcvy9PY3T4frKvniNyf	0.0238616	1533.27054
4/26/24 5:47	Remitano	BTC	25ae9f834ea82f7e07a01aa02d061ef86fbfa21b6c16cc2fe3ceaae0801e31ad	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	38ZWvd5Be2PqMu5xcvy9PY3T4frKvniNyf	0.10593255	6831.43019
4/26/24 9:53	Remitano	BTC	62df4887bd47d4f8d54958d89a6840a0410050a330f95f0586838a7356094d18	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	3M5RWiGdcEDRseLUqaG15HgPLL7bf3644A	0.01397335	901.4134
4/26/24 11:03	Remitano	BTC	3e96d1f215da3dcbcdf5fdabbaa6a44949736bfd6ca6588cd58494f954b63028	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	38ZWvd5Be2PqMu5xcvy9PY3T4frKvniNyf	0.0716741	4614.6072
4/26/24 12:26	Remitano	BTC	d9e87eb25d65dd609657aac1dd39f8cf3bd96b6dfb2315b1478b3f3d229ee6e2	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	38ZWvd5Be2PqMu5xcvy9PY3T4frKvniNyf	0.08341163	5355.74732
4/26/24 13:00	Remitano	BTC	656a90f118fceb58b3e9bd8e546d0184beb9bab250c39f5811451 1b1605a7b9a	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	3M5RWiGdcEDRseLUqaG15HgPLL7bf3644A	0.01882622	1208.80598
4/26/24 13:20	Binance	BTC	f4a9fd1a7606003f0c5a0352c01c6a33a41b0cc3a057a86bf155cd6b0fff04c2	bc1qsfw593j8phg20vvk6cunwdw8w2vyle9146lamj	13mLDAfVfyzD8Vf6x9YZ5pALc3g8TXqPix	0.17209098	11026.6022
4/26/24 15:27	Remitano	BTC	8e7dec54c4dbebafe0e9f395e873f2884e2958447052909cf21871a9d2368752	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	3M5RWiGdcEDRseLUqaG15HgPLL7bf3644A	0.02803407	1786.97292
4/26/24 18:25	Binance	BTC	bac90d1e542d4cdcab9d18f5621a138aa35c35bde4d5d034774b09245567c6db	bc1qsfw593j8phg20vvk6cunwdw8w2vyle9146lamj	1MUxDUmHAVskKATJDCWgk8SJ9ZBHreZAbh	0.01563457	1008.24981
4/27/24 9:36	Remitano	BTC	0e8858122ca89936e34a020a6b3a67c36869dbb5815e165d45c48f2b6f0ea3f8	bc1qsfw593j8phg20vvk6cunwdw8w2vyle9146lamj	38ZWvd5Be2PqMu5xcvy9PY3T4frKvniNyf	0.2542922	16016.32721

4/27/24 15:23	Remitano	BTC	345b0981a8657ce44b2a4074338fd5c8743077a66fe6d7bd4aa7bdf760bf3a7f	bc1qsfw593j8phg20vvk6cunwdw8w2vyle9l46lamj	3MoVdQzjhYJrz9umg4v1oBRRz5pe9kZVcu	0.00665793	420.57811
4/28/24 6:14	Remitano	BTC	e7c697d7bd355cc554184feedd5baee3220c735f1e66b71efcb384a2bd484160	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	38ZWvd5Be2PqMu5xcvy9PY3T4frKvniNyf	0.05324745	3377.72217
4/28/24 9:02	Remitano	BTC	37266a1cd02e3f0d9ff8094acc7c3979e6b4c22dbf66bf39f84c40a46c33a531	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	3M5RWiGdcEDRseLUqaG15HgPLL7bf3644A	0.01456955	930.6016
4/28/24 10:39	Remitano	BTC	a54a83083612d2c3d262c65bc119eefcfba21387a76541e6fdc5bb9267e113e7	bc1qsfw593j8phg20vvk6cunwdw8w2vyle9l46lamj	3M5RWiGdcEDRseLUqaG15HgPLL7bf3644A	0.06339383	4043.50128
4/28/24 17:02	Remitano	BTC	4a54dcb2f5706a06d3589e0e9c043abfd60f45b71e246678c33a1988a7e0e32a	bc1qsfw593j8phg20vvk6cunwdw8w2vyle9l46lamj	38ZWvd5Be2PqMu5xcvy9PY3T4frKvniNyf	0.10447732	6641.5689
4/29/24 6:44	Remitano	BTC	afa85cf850589d7f33ac2b84614b2a5643c6a7e31e9b750a37c8ce3cf9734900	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	3M5RWiGdcEDRseLUqaG15HgPLL7bf3644A	0.01845554	1149.94274
4/29/24 9:09	Remitano	BTC	829908b95ef1f3719e76187dd1cc9f0dc76e2f5060cc51fd27b97de3b6cc832a	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	3M5RWiGdcEDRseLUqaG15HgPLL7bf3644A	0.02714818	1694.17131
4/30/24 12:58	Remitano	BTC	ec4f748a3bd48202b8974b09e5973568c39427c97f3805fb260b1b752ae00cc2	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	3M5RWiGdcEDRseLUqaG15HgPLL7bf3644A	0.02052824	1310.67762
4/30/24 17:20	Remitano	BTC	28f2a2860e85d1374193a54fbca79d1b3db502563e99f9560035b18f39dbb0bf	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	3M5RWiGdcEDRseLUqaG15HgPLL7bf3644A	0.03503483	2107.39232
4/30/24 18:56	Remitano	BTC	47f2dd4cd167345a0ddc3c291124738b6e97b73eb9f25a5cb5ab3595310c8c30	bc1qsfw593j8phg20vvk6cunwdw8w2vyle9l46lamj	38ZWvd5Be2PqMu5xcvy9PY3T4frKvniNyf	0.06700114	4040.91714
5/1/24 7:06	Remitano	BTC	7cc30b30a6290fdf12ffe49d50a2531dcd562d0a4a271ef6c5f89e4cc1c16633	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	3M5RWiGdcEDRseLUqaG15HgPLL7bf3644A	0.02569763	1533.46136
5/1/24 10:42	Remitano	BTC	65e06b604c94be15e0ee67b551220fc3370eed5c96c6939e89a6ed0e2d22604f	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	3M5RWiGdcEDRseLUqaG15HgPLL7bf3644A	0.01802482	1034.25858
5/1/24 11:47	Remitano	BTC	adb433d963c0a25c7edabe916d99c0b8a69ebda6306f3158cfe296ac8467578f	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	3M5RWiGdcEDRseLUqaG15HgPLL7bf3644A	0.02538592	1539.24911
5/1/24 16:57	Remitano	BTC	b56ddbd318bf63d445c681a96090fb81912f01a6a9c8e9908c22e3d166b7c71c	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	3M5RWiGdcEDRseLUqaG15HgPLL7bf3644A	0.01196738	680.86637
5/1/24 19:03	Remitano	BTC	a94764cd0cef9d61d7a68631c991d3a4a6ee19317cc388bd18f57ec68ceaf306	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	3M5RWiGdcEDRseLUqaG15HgPLL7bf3644A	0.02031441	1231.74333
5/2/24 7:31	Remitano	BTC	a9c2eb5684ae94cf40e307dda8ecb09ad5033cf913152482f483f4896edc9d96	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	38ZWvd5Be2PqMu5xcvy9PY3T4frKvniNyf	0.06475934	3733.24449
5/2/24 9:25	Remitano	BTC	fb22d20a19eeb17a4398241fd42747138a1aa0b853e9b7f4fc06404d9523137c	bc1qsfw593j8phg20vvk6cunwdw8w2vyle9l46lamj	38ZWvd5Be2PqMu5xcvy9PY3T4frKvniNyf	0.27315496	15787.01277
5/2/24 16:05	Remitano	BTC	bce267e61020208173db85e0e9b8bd4b82e7ae0bb18b42f544a3b8966b75132d	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	3M5RWiGdcEDRseLUqaG15HgPLL7bf3644A	0.02935892	1738.8434
5/3/24 6:59	Remitano	BTC	c622b96291947c008d41ab7c3524c9f4a8abb7e9f88d3f1c94f7eb767b6e74e0	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	3A3NqjhLiexUzcfgGuVo19uzux8rnbqSVE	0.02254	1331.74998
5/3/24 11:37	Remitano	BTC	a5510b086201d8bcea908961f01b68c4323cf16b563fb6df5c4cdd6e72be20c5	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	3CaPngqFGiu8kSLEcp9uM5JvK97RdAGHBU	0.02945679	1740.42056
5/3/24 16:39	Remitano	BTC	0e29589888eef3117c5abbcfcf0da65c1ea3a0c59f58a3a6b16735212eea1675	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	3KE6diBJr2yCcd9HEUxH5KNd86s2tzPW2N	0.01216447	752.90272
5/3/24 18:23	Remitano	BTC	87a1ab0bc25e8dc3a268c1ed3b381fab8dda62c918df67b2ea7397c33e94e235	bc1qsfw593j8phg20vvk6cunwdw8w2vyle9l46lamj	38ZWvd5Be2PqMu5xcvy9PY3T4frKvniNyf	0.07352273	4344.00595
5/5/24 16:50	Remitano	BTC	705593389ae72ac5b58e774eb670802d182ad0d075a463e1a8b7fb83a3d72023	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	3B9GDHG6WgrWeavz247zAvbd5WrC8rYF7y	0.00765139	491.83625
5/5/24 18:50	Remitano	BTC	2ac6010e319f676cc2e0b0fc8b1f684a90ecf209b0031184c97531a0826c340b	bc1qsfw593j8phg20vvk6cunwdw8w2vyle9l46lamj	38ZWvd5Be2PqMu5xcvy9PY3T4frKvniNyf	0.0579504	3716.27628
5/5/24 22:32	Remitano	BTC	11387e7eac918938afd45ac004e3d95fbeb685c2e985ffca2ad23895205ddaa0	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	38ZWvd5Be2PqMu5xcvy9PY3T4frKvniNyf	0.02634208	1683.37771
5/6/24 21:32	Remitano	BTC	f13bb22e0432ff5c236db64e1b45c62221e2f59ecf0a1d24e507d3826d00c019	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	38ZWvd5Be2PqMu5xcvy9PY3T4frKvniNyf	0.03151618	2000.35495
5/7/24 7:35	Remitano	BTC	38eb311b6ee9e86f9c0cb082b4b1fb1548777a32ed42a4b38d2c64feefca2c6c	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	3KKGPBqG2GW5PNVmktjoJwsSoGmfrvVTBB	0.03217305	2047.80659
5/7/24 10:56	Remitano	BTC	03bbe10be0cd51bae67fcb37a18d14437ad7488b70ce847966fae3f03b794202	bc1qsfw593j8phg20vvk6cunwdw8w2vyle9l46lamj	3KKGPBqG2GW5PNVmktjoJwsSoGmfrvVTBB	0.05660285	3623.5554
5/7/24 11:50	Remitano	BTC	3fade7b6109d3e1171956ba4de8aa7620c0a7554a4e1287fa78f0af1635fb724	bc1qsfw593j8phg20vvk6cunwdw8w2vyle9l46lamj	3KKGPBqG2GW5PNVmktjoJwsSoGmfrvVTBB	0.01837721	1160.85969
5/7/24 17:23	Remitano	BTC	7b136e5fa864cce5d2e36d0049244d0e890672e6eb98ac58cfde8e06be75be07	bc1qsfw593j8phg20vvk6cunwdw8w2vyle9l46lamj	3KKGPBqG2GW5PNVmktjoJwsSoGmfrvVTBB	0.05701505	3634.9546
5/8/24 7:02	Remitano	BTC	58635e7c4b805f9c9f9e67bcd6691ebc5a1f4ead83ddab4524970e8d271aaff2	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	38ZWvd5Be2PqMu5xcvy9PY3T4frKvniNyf	0.05764345	3589.34926
5/8/24 10:47	Remitano	BTC	7e3d6d7a504d40e8bbe8b4fb2ce3420411a3dad49bf059666e67099dd6dda971	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	3G1gfTQn81jgaPUCWCoSr8j17AtiWn17uy	0.01600216	995.52894
5/8/24 12:51	Remitano	BTC	41d652a2aeef5664bcc88672d91e02f19de404d31fd093ddd872895e9a758515	bc1qsfw593j8phg20vvk6cunwdw8w2vyle9l46lamj	3G1gfTQn81jgaPUCWCoSr8j17AtiWn17uy	0.08639183	5393.1629
5/9/24 6:36	Remitano	BTC	1a19550afb9c440acf82a54a93e456e8e85f1b17b749ad5752b944f18530c28d	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	3DGPG9Lh6iLSkxYf9UZxzxjcUKo36xUva9	0.03101634	1915.32909
5/9/24 6:36	Revolut	BTC	90d55dd285f1d688b00625a5bd5c80c643483f4db00b7c7861892713ed3f7a17	bc1qsfw593j8phg20vvk6cunwdw8w2vyle9l46lamj	bc1q7gku9m33re89mes97dwq4lawwxg3hj6g28umcy	0.11337991	7001.46568
5/9/24 8:01	Remitano	BTC	9851a7f200d9c038b4fef19a02b544bc90d782c98fb14d1d41e31194d7a49c41	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	3D8JCs231iJxK8Jx86pJ4TAWrAAtbRxRPW	0.01620206	995.73859
5/9/24 8:24	Revolut	BTC	5f713dec365ccc4e651ade4658e4fb7407edaf3b56d8ecd7149dca99cdfcba66	bc1qsfw593j8phg20vvk6cunwdw8w2vyle9l46lamj	bc1q7gku9m33re89mes97dwq4lawwxg3hj6g28umcy	0.08157585	5013.45025
5/9/24 9:34	Remitano	BTC	f6518e683e3218aedf6ecf474e76960f9f41511d70e0ef15479279e294cb1069	bc1qsfw593j8phg20vvk6cunwdw8w2vyle9l46lamj	3G1gfTQn81jgaPUCWCoSr8j17AtiWn17uy	0.03640357	2234.17919
5/9/24 12:34	Remitano	BTC	e1bfcb823d31b851ac82e3f108d8c7b9e7227012ddcaed74c2b6c73edeeedc9e	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	3D8JCs231iJxK8Jx86pJ4TAWrAAtbRxRPW	0.03043682	1862.11886
5/9/24 12:41	Revolut	BTC	08e2004bb90043f78c8f3e5b61fadf1a2489d4fccb5c47a30656a1a4d038cd06	bc1qsfw593j8phg20vvk6cunwdw8w2vyle9l46lamj	bc1q7gku9m33re89mes97dwq4lawwxg3hj6g28umcy	0.08146762	5003.82676
5/9/24 14:54	Remitano	BTC	28bf9da3ee010ac2c9d9bd051c45e16628de4b9f9eefbca0d23c3238406e089c	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	3D8JCs231iJxK8Jx86pJ4TAWrAAtbRxRPW	0.00974534	598.64211

5/9/24 22:23	Remitano	BTC	98c4421d5f95dab48c29788f98f673c4d99f2cbf1037fbb84e467d40f1822eae	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	33heGnSTbA6U7WrfMBYoWYgCRBek2MrKTA	0.01322861	827.6546
5/10/24 7:25	Remitano	BTC	9b0dd5e7961ffd237659ab1971686c58be5a513eef2c707a4fba6cd1863f8bc2	bc1qsfw593j8phg20vvk6cunwdw8w2vyle9l46lamj	38ZWvd5Be2PqMu5xcvy9PY3T4frKvniNyf	0.11200744	7094.08978
5/10/24 11:58	Remitano	BTC	278ec91989658fd801f6e92d8e2ad93cb987abd08ee5855ae36ded6e692daaa8	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	3AymDrgNq3WQZaNLh4vxLe8bxVzGaHqQhz	0.01900458	1197.6692
5/10/24 12:39	Bybit	BTC	ce61abdc06bf14d046ba5362c96ba392ada514519eea23f104a73f2996258981	3KnqtxBsSywJ4ptqaQ56QWNh1JaTkDrkw8	14rxMsRQV5fkTDb3ShorD91xQvdwp34hjb	0.57545563	36265.23107
5/10/24 13:55	Binance	BTC	12f25da1eb739e4e76c24e523d2f395fa144bf83d6936685b3853e23fd3af2c7	bc1qsfw593j8phg20vvk6cunwdw8w2vyle9l46lamj	1DMhMwn4apg49oVjRpbaZqJDDLJaN6iqox	0.00237987	149.98157
5/11/24 8:04	Remitano	BTC	af5e71aea106aa6b18c6729023e57ed1377fdbbc987dd1fb727c550373f283e2	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	3AymDrgNq3WQZaNLh4vxLe8bxVzGaHqQhz	0.03115467	1898.91764
5/11/24 8:08	Remitano	BTC	5a6e141d4fc46971ce45a03c0a373212bb903e0e603c5f55acec6bd50e061ac3	bc1qsfw593j8phg20vvk6cunwdw8w2vyle9l46lamj	31jJbyCxErbbfkuGP1dtz2Pz9jt9SWNv83	0.01641318	1000.40466
5/11/24 14:01	Remitano	BTC	5182cb88286c591e58b18e7c2bbc929ed3ec98cff917a1302212f302789deb15	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	3AymDrgNq3WQZaNLh4vxLe8bxVzGaHqQhz	0.02796018	1701.35822
5/11/24 21:56	Remitano	BTC	77224d472b7487918b01175f148cf9d267da5f0bf5fef8186cf27dbc6f0b5d24	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	3AymDrgNq3WQZaNLh4vxLe8bxVzGaHqQhz	0.01801163	1096.17501
5/12/24 1:51	Bybit	BTC	c112147033e10979afbb346573e4b09026261f9e28601733b9ee88dc77d844aa	3KnqtxBsSywJ4ptqaQ56QWNh1JaTkDrkw8	14rxMsRQV5fkTDb3ShorD91xQvdwp34hjb	0.71452037	43459.40822
5/12/24 13:31	Revolut	BTC	db8a5298e0cf978b64e149a3b65d0fb57fccd3bb57a67dd0be34abc4bfb6ed66	bc1qsfw593j8phg20vvk6cunwdw8w2vyle9l46lamj	bc1q7gku9m33re89mes97dwq4lawwxg3hj6g28umcy	0.06544229	4001.80192
5/13/24 7:05	Remitano	BTC	80abbede5e2557f095a9f700d04cfa8f87d58f6bcd87c1b1da761d5259973a22	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.03364662	2059.42617
5/13/24 10:12	Remitano	BTC	67a58704451aa699e61dd53c36eed3919ccd23f4375a636007c1cbe417cbb1a0	bc1qsfw593j8phg20vvk6cunwdw8w2vyle9l46lamj	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.02439771	1532.42724
5/13/24 14:47	Remitano	BTC	3472b444e86a4519cf395efc4a787cb5b09e08b6b128ed0dde2e23acb3da5857	bc1qsfw593j8phg20vvk6cunwdw8w2vyle9l46lamj	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.0600254	3776.54126
5/14/24 20:58	Remitano	BTC	f73b32c368cfed7b5946e7897d99696b005837ca9a6e9e8626d7dc2ba452045e	bc1qsfw593j8phg20vvk6cunwdw8w2vyle9l46lamj	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.17355924	10688.5972
5/15/24 13:52	Remitano	BTC	2f13ee5fbc5a18ae629437bb1d522e8a485d5a4ac1a203c7f498976bed1c5599	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.01910335	1230.58737
5/15/24 14:22	Remitano	BTC	d71ed0b62b9cce439ac2559473ce5e48478725493ab677d1cd096523cd608dd2	bc1qsfw593j8phg20vvk6cunwdw8w2vyle9l46lamj	38ZWvd5Be2PqMu5xcvy9PY3T4frKvniNyf	0.11982337	7718.70516
5/15/24 23:28	Remitano	BTC	4191a41057cdcf48000c3881ebdea62a86a28f4b44b9bfb7646148cedcced5a1	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.00810979	537.1281
5/16/24 14:16	Remitano	BTC	4224db7b492ed62b38046962bfed603f2b9d43d8fd6261ce7ead6651ea0a09ba	bc1qsfw593j8phg20vvk6cunwdw8w2vyle9l46lamj	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.04915658	3253.28029
5/17/24 7:28	Remitano	BTC	77225cc0d394724b870de3cf89a86cc42ede492267e752ff7828f659b7982279	bc1qsfw593j8phg20vvk6cunwdw8w2vyle9l46lamj	38ZWvd5Be2PqMu5xcvy9PY3T4frKvniNyf	0.06168819	4074.42722
5/17/24 8:03	Revolut	BTC	b47577d0da10ce4281e2fab8d8a5596042f16cf9bb516951248852967e77765b	bc1qsfw593j8phg20vvk6cunwdw8w2vyle9l46lamj	bc1q7gku9m33re89mes97dwq4lawwxg3hj6g28umcy	0.06047627	3946.10867
5/17/24 14:56	Remitano	BTC	d8069d850f7641fbe266a3e5e2d1eedb1475e81ba676de5a5e0c57fb5c3296f8	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.03552493	2350.13789
5/18/24 11:35	Revolut	BTC	5623e9cb5a4b03e0be5e2dd8c717a7183125ccf28513570011761bef95f9df75	bc1qsfw593j8phg20vvk6cunwdw8w2vyle9l46lamj	bc1q7gku9m33re89mes97dwq4lawwxg3hj6g28umcy	0.04457165	2988.5893
5/18/24 17:54	Remitano	BTC	30cd89d914d4e5a5d70fa0f736ad3977af765a0f90680c1de6f89f44459e877e	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.00747814	500.41013
5/18/24 20:10	Bybit	BTC	722c13952b81f8c22bbd59f990d81b18d7405453fa8db53318b1ff9261e575d5	bc1qaj9tzy4g34pf8kp9f8rufdnt54zxck4wuljstd	1HyTkypyP8yoRGSRrvr74SyEhhX1bkLMiQ	0.02980146	1992.92585
5/19/24 9:05	Remitano	BTC	820ae9edae2676c8603dc8e5276f28ed39b861dae24d9421880a2b9af28d7ff0	bc1qsfw593j8phg20vvk6cunwdw8w2vyle9l46lamj	3BjbZnAwmmxvQFnibcyGRd8SAwM6xTLYpA	0.00297278	198.96091
5/19/24 13:57	Remitano	BTC	d92abea636adfe80ad52aaa5b78349aa0dd569a88762a94d380760f9a13d7f2c	bc1qsfw593j8phg20vvk6cunwdw8w2vyle9l46lamj	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.03577459	2392.29942
5/19/24 23:24	Remitano	BTC	1fb9a75adaf536e3f286525f78633340854f27fb41b8150165f94a3ff44c635b	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.00729186	484.11781
5/20/24 16:48	Remitano	BTC	66ad237f48660b5edce92a7accc8d05e1d0026dc41f8b432f792d5a27ebeb124	bc1qsfw593j8phg20vvk6cunwdw8w2vyle9l46lamj	3CZ6NHrctR8ceWwyYyJQXP96PMAqEs5J4a	0.00220211	148.98065
5/21/24 10:31	Remitano	BTC	db4b1055b265c2769947ee4e275738823859a06aa75bacca1bc93e18648a17de	bc1qsfw593j8phg20vvk6cunwdw8w2vyle9l46lamj	3KSpJdiRmej8XkqCYswa58pff127b7nQxc	0.00702608	500.38063
5/21/24 16:46	Remitano	BTC	97a2e0633673924a202a395a800eb7ab9912a5fcff53db5c749ef9bd22596bd6	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.04296702	3004.21408
5/22/24 5:47	Remitano	BTC	2d74b8972d78feec49918100fade80baf8f0187dda5506e025828851939a6a81	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.03490036	2426.98569
5/22/24 6:52	Remitano	BTC	c281ffef00bd9906953a2feef29a9f30a01f4d9825f6d73757ae1820d7752958	bc1qsfw593j8phg20vvk6cunwdw8w2vyle9l46lamj	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.0159691	1115.83687
5/22/24 14:38	Remitano	BTC	41b8200628ccb7599b1ae2c515fcf89ae96038749df5f7b23c629dc7efde5aea	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.00481127	334.67088
5/22/24 14:46	Bybit	BTC	0455f5a6f39dbc24628bce15ffd43354fe9a61e5165f53f39c5dafd8512c256e	bc1qaj9tzy4g34pf8kp9f8rufdnt54zxck4wuljstd	1HyTkypyP8yoRGSRrvr74SyEhhX1bkLMiQ	0.38675781	26902.78818
5/23/24 8:39	Remitano	BTC	9edd533b4779a69dccfb801aae7c86d66e201774a8fda542775a97a9139fd8ca	bc1qsfw593j8phg20vvk6cunwdw8w2vyle9l46lamj	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.05078329	3540.14377
5/24/24 7:33	Remitano	BTC	d3a183dee10b7010ed0fa5e0bffd69d6284c40d92688a2e8940fdfa1ca17a014	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.00924845	620.74792
5/24/24 7:56	Bybit	BTC	45d56a769315c53771bc3be1ce2b63caad12fc68d8377e2a8bfa3a4c5ff2db32	bc1qaj9tzy4g34pf8kp9f8rufdnt54zxck4wuljstd	1HyTkypyP8yoRGSRrvr74SyEhhX1bkLMiQ	0.01489025	1011.73814
5/24/24 10:23	Revolut	BTC	f2ebcadb3c047c08f58ca1c82c90ab7a6b028cef65b3e84db6a7688ec0bfeb72	bc1qsfw593j8phg20vvk6cunwdw8w2vyle9l46lamj	bc1q7gku9m33re89mes97dwq4lawwxg3hj6g28umcy	0.0148512	1001.16617
5/24/24 12:07	Revolut	BTC	81375fda4a21514a61084420bf35c6408ef616fb7c6a37a07c5b8f341db97762	bc1qsfw593j8phg20vvk6cunwdw8w2vyle9l46lamj	bc1q7gku9m33re89mes97dwq4lawwxg3hj6g28umcy	0.0148525	1009.17316
5/24/24 16:49	Remitano	BTC	c68c58816f9e184e5287b73fedabcc0e309f7091c402e40c366e0fb9e5a63708	bc1qsfw593j8phg20vvk6cunwdw8w2vyle9l46lamj	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.02493971	1701.5995

5/25/24 14:07	Remitano	BTC	39bc0950c2d3e12ac4b1fde00c8aee05427a9464ac5c612fab2bf459636a4267	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	38ZWvd5Be2PqMu5xcvy9PY3T4frKvniNyf	0.05333073	3691.11582
5/25/24 16:47	Remitano	BTC	36a2f0b2468751672075e4d0c839a4a4536bbafa81c8f2c917ccd29099e6f4f8	bc1qsfw593j8phg20vvk6cunwdw8w2vyle9l46lamj	3KSpJdiRmej8XkqCYswa58pff127b7nQxc	0.01450415	999.76874
5/25/24 19:06	Remitano	BTC	ed0a495a2594bd1beaead5d4760f0558d157542b124d1aa47066318c381f3d6d	bc1qsfw593j8phg20vvk6cunwdw8w2vyle9l46lamj	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.02583751	1787.95259
5/26/24 9:10	Remitano	BTC	9eac5df7b8c5e3e4ac44861812ecfb267fb3fe51ceaf2cf7035a40c2654a855e	bc1qsfw593j8phg20vvk6cunwdw8w2vyle9l46lamj	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.04214998	2920.52786
5/26/24 10:27	Remitano	BTC	ad91b4ce4e0532a7458d33b2d2c766b9aa8450811b38ef15933007ab0f95a80d	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.01427574	986.59825
5/26/24 19:24	Bybit	BTC	cd865c1db83554ab17748484c4bfbf29177fb038417cfe0cd6f16ce2d26ceb84	bc1qaj9tzy4g34pf8kp9f8rufdnt54zxck4wuljstd	1HyTkypyP8yoRGSRrvr74SyEhhX1bkLMiQ	0.00123414	84.87745
5/26/24 20:31	Binance	BTC	f03c348ddc0280f1e02c6599e274af83e457b0cbe076c71c5f642706a5bbf5d1	bc1qaj9tzy4g34pf8kp9f8rufdnt54zxck4wuljstd	13WWx7qQ1QBoY2E3sjaRrzvWzg2JJkDAgg	0.03708371	2553.26127
5/27/24 17:44	Binance	BTC	13fd1ca203012db8e63c2c4f69869114d31a78f060b6b6947d6adc93ba6f4b99	bc1qaj9tzy4g34pf8kp9f8rufdnt54zxck4wuljstd	13WWx7qQ1QBoY2E3sjaRrzvWzg2JJkDAgg	0.00854858	600.16845
5/27/24 18:43	Binance	BTC	a3836f5790ef41277d9cb36bf31cd20f876adf8e668535507422c4a8a587b035	bc1qaj9tzy4g34pf8kp9f8rufdnt54zxck4wuljstd	1PvjGd7aCpvRzZtz4kL9YgdvnYPdpm16oj	0.0042851	300.59912
5/28/24 12:41	Remitano	BTC	7f1fe274e77db6777b5cb2b3ce4c6087bb8bc48d7a0e65bb9d30716e58ef222b	bc1qmz2rj0nhr7u3ruzusuxtfd979j2rpfed3relgg	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.88002085	60269.72395
5/28/24 13:37	Remitano	BTC	32e038c3d65d2a93ace31734a3b6c3c3c96d752a3dac87b46ff6b8042155276b	bc1qsfw593j8phg20vvk6cunwdw8w2vyle9l46lamj	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.02802077	1944.2724
5/30/24 1:06	Remitano	BTC	dfe3e4f13b7133b0d0bbd11b1c9dc3f7297a48aa3a3bae65b6295ab381ff2b53	bc1qsfw593j8phg20vvk6cunwdw8w2vyle9l46lamj	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.03212221	2166.14099
5/30/24 8:13	Remitano	BTC	615adf1d949d2e3f5d8b8a9b5028359a627f96cc4c2133f9b7cd08f00e29c177	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	38ZWvd5Be2PqMu5xcvy9PY3T4frKvniNyf	0.04764274	3218.65061
5/30/24 20:37	Remitano	BTC	56aa4c438477752443b5fcf5a044952366b5c52bbcd12db82f1aab9c5b724867	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	38ZWvd5Be2PqMu5xcvy9PY3T4frKvniNyf	0.06123312	4137.93892
5/31/24 10:33	Binance	BTC	2c4cf6c4075938d414ca071f8e2ef3ed80ae91e143f94c9cf5cdb87c86435105	bc1qaj9tzy4g34pf8kp9f8rufdnt54zxck4wuljstd	13WWx7qQ1QBoY2E3sjaRrzvWzg2JJkDAgg	0.00293532	200.00892
5/31/24 17:57	Remitano	BTC	69a5bad1fdc404a75cc250b34cf157249352b81e7f5808fb0f34e9a84d3dc1cd	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.00804688	541.85702
6/1/24 12:41	Remitano	BTC	e854c640dbe2a05b6389f1353b415e53adc6013f56b1c7c03f763c81e117a4c7	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.03571366	2410.03813
6/1/24 13:54	Remitano	BTC	e98655dfc14f2e5138d8177a8e13acaec962fe4c49ebe59f395d4dda8789719f	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.02986314	2023.35883
6/2/24 10:22	Remitano	BTC	d5067a9e08caab89456d1eea1f555d3b5ba8ee55c95349529d72500197b2be48	bc1qsfw593j8phg20vvk6cunwdw8w2vyle9l46lamj	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.02817465	1908.03238
6/3/24 12:22	Remitano	BTC	5e489d6f85c2754e6416137c5e381964e7469d7300af1c78e9bce2141ab955b2	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	38ZWvd5Be2PqMu5xcvy9PY3T4frKvniNyf	0.83273082	57571.9611
6/3/24 16:32	Revolut	BTC	f64a6a2c69ce2f181c7990c236e400fbe8ec111f45548f2988e4150cd7e5df00	bc1qsfw593j8phg20vvk6cunwdw8w2vyle9l46lamj	bc1q7gku9m33re89mes97dwq4lawwxg3hj6g28umcy	0.01061303	737.86391
6/3/24 21:04	Remitano	BTC	f024eaeeff204821610fc40c38cf016d583aebc9548ad264ea4f64bf213c7b3f	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	38ZWvd5Be2PqMu5xcvy9PY3T4frKvniNyf	0.078754	5459.69902
6/5/24 17:48	Remitano	BTC	c5a810593e79eff639d7aece2ecb77cb139f64571052bf66d2d4a54b24565b6a	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.01398005	1000.02821
6/6/24 10:43	Remitano	BTC	5849cafc9190e6e202d4783becae2fc766f8be92d9ab1bcbaf0d84b051bc704f	bc1qmz2rj0nhr7u3ruzusuxtfd979j2rpfed3relgg	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.02113403	1498.86831
6/6/24 15:43	Remitano	BTC	3c685e658d116174fb39c007b7f262f182a214abfd1c41110c9d10480af436df	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.02517617	1799.59867
6/6/24 21:29	Remitano	BTC	7615ba18a3f48eba8d3f0accc9b20fc81557b30d6bae19ef71944e772631a327	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.01130688	804.11907
6/7/24 17:24	Bybit	BTC	d0137332f06a11f80f3b734890797c210632f2ddddbc936c02863094ad5f4bc7	bc1qaj9tzy4g34pf8kp9f8rufdnt54zxck4wuljstd	1HyTkypyP8yoRGSRrvr74SyEhhX1bkLMiQ	0.01418287	1007.16049
6/8/24 8:35	Remitano	BTC	37b40e648009f81b9b25b34ea4edf5f3d897bd34b6c216e759c470dbe2262c8b	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.02565029	1781.75174
6/8/24 21:48	Remitano	BTC	578bc28df3c5a5f418fa0cfbc8e755c6a0c8107f10d965590ec36c8235da0a88	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.00504299	349.67659
6/9/24 19:40	Remitano	BTC	03cfb8db1bbfc901a9a4578dfaff7c2738f8bb9a94ebce7ecd040266ad0a860a	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.0222052	1549.63163
6/11/24 7:01	Remitano	BTC	be9604e926983d77581a5ff9c40a13553da35f1ae03c027dea3678dc9cadb3c7	bc1qsfw593j8phg20vvk6cunwdw8w2vyle9l46lamj	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.02338766	1587.81233
6/11/24 12:51	Remitano	BTC	a23f64bb181cfc20645e88fd7b67201c4f527802c6755e78e08647ace6a1cf58	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.01493539	998.06998
6/11/24 14:27	Remitano	BTC	5c155daebac0893c0fd195b6563acbb54ca58a42b404112c0f441be298cd368d	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.01420257	953.60799
6/11/24 15:58	Bybit	BTC	a66c5c76fa05bb4788f768439ad088b522f3032e11a6941c79223d343d9cb5a3	bc1qaj9tzy4g34pf8kp9f8rufdnt54zxck4wuljstd	1HyTkypyP8yoRGSRrvr74SyEhhX1bkLMiQ	0.00905045	604.76826
6/12/24 9:46	Bybit	BTC	a3911bd16997e1ed6364d505d776636aa673a9726eaf16fe1d93488982294ae4	bc1qaj9tzy4g34pf8kp9f8rufdnt54zxck4wuljstd	1HyTkypyP8yoRGSRrvr74SyEhhX1bkLMiQ	0.00237209	160.13299
6/13/24 8:07	Remitano	BTC	734b4edae177212a49e7de7c26dcab076d37b1930cf73e292c98e2907a81dfb2	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.01267678	858.28595
6/13/24 9:24	Remitano	BTC	447a2946b02a9b5b83bdf420e9e6f7f89d85ac58fb0e42bd91b9b1a4f932d3ee	bc1qmz2rj0nhr7u3ruzusuxtfd979j2rpfed3relgg	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.0074056	500.03641
6/13/24 11:18	Revolut	BTC	3c520c4973b3bf64fb4e238f972db956c8a8e058c03a3cd5fd4e6c1b37900728	bc1qsfw593j8phg20vvk6cunwdw8w2vyle9l46lamj	bc1q7gku9m33re89mes97dwq4lawwxg3hj6g28umcy	0.01921811	1304.78648
6/14/24 15:12	Remitano	BTC	2aa8effffa05269ce23f899e9bc4e6cfbe53a9960f7cfe40b2b2c51846f67ec0	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.01498452	1000.10493
6/15/24 1:31	Remitano	BTC	4539e23258ca778c4726d2950716cf265b0953d1719ca9a2b91e76f471d9e7bf	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	38ZWvd5Be2PqMu5xcvy9PY3T4frKvniNyf	0.04627828	3057.82439
6/16/24 16:03	Remitano	BTC	fd7b983001b069423cde42c63ab20e0cb6f0b331b9ae360f8e25b41b3ec5e5ac	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.0392414	2614.53087

6/17/24 14:44	Remitano	BTC	53c0eca28938acedbd6780eeef4a895e1c8eea5f041db858aebd14b78a4323dc	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	38ZWvd5Be2PqMu5xcvy9PY3T4frKvniNyf	0.05673432	3780.29795
6/18/24 9:53	Revolut	BTC	5f31ff883e8f4d7530e444cecef822a6308b10591963d4e7eaf4b49ae913ee09	bc1qsfw593j8phg20vvk6cunwdw8w2vyle9l46lamj	bc1q7gku9m33re89mes97dwq4lawwxg3hj6g28umcy	0.00860371	571.98953
6/18/24 16:20	Bybit	BTC	4f8833b84bcd7918bbe7371cd66ca0c0b0f1f5efdfd53041060c5a2de2a3e992	bc1qaj9tzy4g34pf8kp9f8rufdnt54zxck4wuljstd	1HyTkypyP8yoRGSRrvr74SyEhhX1bkLMiQ	0.01550897	1002.13303
6/18/24 16:42	Remitano	BTC	25b2464ed5e181e55c264736f24d1e95b1c75b35c8542f2c876b2653444b090b	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.00800205	517.06326
6/20/24 10:47	Remitano	BTC	1df211391670111fc3480cf8f7e2e53d4a4a85749f7a601a7f732a6e7b25077a	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.03986819	2623.2372
6/22/24 15:37	Remitano	BTC	27cc0fb930fe3cecd20c411fece236b79d2d927445802d01c1149ebab59da91c	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.01333112	856.41914
6/22/24 21:29	Remitano	BTC	6907f39e8af771eedb3a45a8f514b354eba1aae70ea7986c005ad127f6956b0d	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.02487833	1595.1821
6/23/24 21:54	Remitano	BTC	7b0cf1308cc1b8800514807a629c8ebc35d66d2dc0438e52ba2a8d35a3320c34	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.01191642	759.08394
6/24/24 17:09	Remitano	BTC	e3f5edd6866776a6b019f301982aa7d80992b1c3abc79a985711f13009f9b505	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.05215388	3167.25506
6/26/24 7:15	Remitano	BTC	d7a7341cddb3d5d34b568b9aba0edb721082a48ab574c7169ec6bac07425bdf7	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.0089816	555.03198
6/27/24 15:20	Remitano	BTC	3c6de918f3d7becf274fc3732877d1eb19ddbce1634864c03b0d28e5c40e2ce9	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.05215815	3225.303
6/28/24 7:22	Remitano	BTC	a69dd4981d19651d9cbc8a5cffd8c2f52a05a203d09ab4c873d8560b7c423215	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.00752187	462.82705
6/29/24 11:50	Remitano	BTC	41cfa3d9b6eef4bd05979d8b4666f8e9108f46a482ed52377df1d79aaf61f744	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.03626441	2215.67567
6/30/24 8:09	Remitano	BTC	8dd27d3abe014845cfa44f1dd58f63c2d090b284b53946725eb2bda3f6d9c057	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.02768937	1686.42939
6/30/24 13:39	Remitano	BTC	41952015df09d2b82b6913068328192f27c6829e49ef6fbb322a999a641eef34	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.04883611	2999.80982
7/1/24 17:40	Remitano	BTC	16e5d025984268421e85cb1bc03524b9f3ac3778755501179bcbe5bed9d183bc	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.01738061	1098.88681
7/2/24 11:17	Remitano	BTC	a03756380bdb24b391155a553fc104aa5093506a4eeb47c26b4dc064db41d70a	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.01517033	949.76748
7/3/24 6:55	Remitano	BTC	fa7d1cabe8409311a727699d3fd5f3f8d41feb2febb80a1a2b1abb6ed0cb9b7c	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.02230867	1362.01502
7/3/24 21:14	Remitano	BTC	49e78bb8daed638a388f7c3e4923d3f91104de843cd11ecb1c18242504cb1add	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.00926556	553.4294
7/3/24 21:43	Remitano	BTC	b2e5cf1a3acd6fb113e2afc223125357fd6594f31dc594704e08ea6482f92168	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.00502811	311.96647
7/4/24 17:27	Remitano	BTC	c18dedcfc8a7df1aa44759fb9f2a151b8d355a5f552ce5caec9a9b15dd667120	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.004345	252.49799
7/5/24 11:38	Remitano	BTC	6846ba9c1c6ff58fffae1d310987a5f48227de3a2f60adf73999cd8716d13bd3	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.01298276	718.03296
7/5/24 16:28	Remitano	BTC	6d8578f57de359885c31eff6ab94e5a29df33635dc659f469fd1696ae8b95e8e	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.01838333	1040.48912
7/8/24 8:29	Bybit	BTC	583e661e4536c49b12a3772abe2a1f4977373e4561b3b3bd09a915fdd220e10f	bc1qaj9tzy4g34pf8kp9f8rufdnt54zxck4wuljstd	1HyTkypyP8yoRGSRrvr74SyEhhX1bkLMiQ	0.00318744	177.59762
7/9/24 8:04	Remitano	BTC	732225d0d955cd9cc32a6812a0f99ecf6d58df9c779b5ec646c7097b573f48b3	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.02453453	1406.6068
7/9/24 13:25	Remitano	BTC	324e84d6f6200d13cad3b9365b4699fac785fa0136812bb92ab3e94d41a4348e	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.0174554	1000.36985
7/11/24 7:35	Remitano	BTC	f32a50166eca698805d7667bbe26e0d79e840c1cb89d91be29288184c6715cbf	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.01718026	998.94519
7/11/24 10:23	Remitano	BTC	01b6266d4c2ab02d730292479ee35631d5c614eac5ab49194f756168f26050f3	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	38ZWvd5Be2PqMu5xcvy9PY3T4frKvniNyf	0.17344817	10093.70525
7/11/24 19:38	Remitano	BTC	29289a4ff88eef8511a2ba35ea18e5025201d641c10f9acf69488d634daad468	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.0069576	402.41993
7/13/24 6:35	Remitano	BTC	1cc097c0bb607c1277bfcaee6dfbcf665209e0f452c20d6469ce64243c4bd522	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.02580708	1499.59445
7/13/24 6:35	Remitano	BTC	8f6523785952be0f24668d13c9559d71ffd6e806aa7462cab6389e3e214ba683	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.04473228	2599.29751
7/14/24 16:41	Remitano	BTC	d7ffb5ac2f922898265aa15de0e64796831c1b8dc4137ebd460a8ab88440c068	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.00687046	413.1176
7/15/24 15:06	Remitano	BTC	718b5fb8107997fc7cfaf2e91d7c14741c19ca13043d885d213f6216de1609a4	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.03551817	2236.47297
7/16/24 14:31	Remitano	BTC	01a1002b9fa01b256b3fbe1d69cdc31cf0f1487aafb613a908d6a3d50bed1d59	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.03386916	2193.55478
7/18/24 13:35	Remitano	BTC	fcda8b36f980ad8d6c07b2ea48b71eb7bc25856eb4d07d211b162e201594ac16	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.01777382	1153.68159
7/20/24 9:55	Remitano	BTC	c8962e07ed03a486f24484d8813043ec55475d6e344938553421582933d281e6	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.03228131	2148.42448
7/22/24 9:35	Remitano	BTC	f47710251a41be6dd01ff3fcfd1093853b2cd1b76f22657507c212070efc90e2	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.03072728	2066.0682
7/23/24 14:34	Remitano	BTC	f8198d7f13dba1eaa333bdbcb6c4803fccf8bbbd4f4fe940047c87006bb6baee	bc1qmz2rj0nhr7u3ruzusuxtfd979j2rpfed3relgg	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.00747821	495.93754
7/23/24 20:16	Remitano	BTC	c963892e22c75ccd7b0d0a48ff3adb1d9e05d51a381b732edb96b8b1bc15ed81	bc1qktalnymfk50wwp4qasyu6v6gxqw2gwu55hjts4	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.02111697	1392.02834
7/23/24 21:18	Remitano	BTC	7087a3ed5f22d312c866e5efa275ece2e0759026545a9f780767f8aac58d3974	bc1qmz2rj0nhr7u3ruzusuxtfd979j2rpfed3relgg	39TPPnjRGB8ANVbs1K7RFoBBDNtvXWtECj	0.007553	496.91799
7/25/24 11:18	Remitano	BTC	4ce5ce38c879a03a202e824152ea5740b7578f9627c6e957d99a40a3c8cd3709	bc1qmz2rj0nhr7u3ruzusuxtfd979j2rpfed3relgg	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW	0.0077841	499.48756

Total Transfers: 200

Unique Receiving Addresses:

bc1q7gku9m33re89mes97dwq4lawwxg3hj6g28umcy
38ZWvd5Be2PqMu5xcvy9PY3T4frKvniNyf
38Ep5mFzh6oNbuFXSL1Hvk3g1TwXUMX8xv
3M5RWiGdcEDRseLUqaG15HgPLL7bf3644A
3A34Ggh1EUNXe4K8ayTLNLdKYAUDTnEU63
13mLDAfVfyzD8Vf6x9YZ5pALc3g8TXqPix
1MUxDUmHAVskKATJDCWgk8SJ9ZBHreZAbh
3MoVdQzjhYJrz9umg4v1oBRRz5pe9kZVcu
3A3NqjhLiexUzcfgGuVo19uzux8rnbqSVE
3CaPngqFGiu8kSLEcp9uM5JvK97RdAGHBU
3KE6diBJr2yCcd9HEUxH5KNd86s2tzPW2N
3B9GDHG6WgrWeavz247zAvbd5WrC8rYF7y
3KKGPBqG2GW5PNVmktjoJwsSoGmfrvVTBB
3G1gfTQn81jgaPUCWCoSr8j17AtiWn17uy
3DGPG9Lh6iLSkxYf9UZxzxjcUKo36xUva9
3D8JCs231iJxK8Jx86pJ4TAWrAAtbRxRPW
33heGnSTbA6U7WrfMBYoWYgCRBek2MrKTA
3AymDrgNq3WQZaNLh4vxLe8bxVzGaHqQhz
14rxMsRQV5fkTDb3ShorD91xQvdwp34hjb
1DMhMwn4apg49oVjRpbaZqJDDLJaN6iqox
31jJbyCxErbbfkuGP1dtz2Pz9jt9SWNv83
35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW
1HyTkypyP8yoRGSRrvr74SyEhhX1bkLMiQ
3BjbZnAwmmxvQFnibcyGRd8SAwM6xTLYpA
3CZ6NHrctR8ceWwyYyJQXP96PMAqEs5J4a
3KSpJdiRmej8XkqCYswa58pff127b7nQxc
13WWx7qQ1QBoY2E3sjaRrzvWzg2JJkDAgg
1PvjGd7aCpvRzZtz4kL9YgdvnYPdpm16oj
39TPPnjRGB8ANVbs1K7RFoBBDNtvXWtECj

Exhibit 1-H

<<< </legacyquote></quote>Once wire hit account let me know, it should already be in account. Maybe confirm from your bank how long it will take
2024/02/26 10:35:49 8:live:ph2corp_2: Okay I'll let you know once it hits.
2024/02/26 13:21:21 David Sham: Bitcoin just hit 54K
2024/02/26 13:21:28 David Sham: I told you 🔥🔥🔥
2024/02/26 16:48:02 8:live:ph2corp_2: Still waiting on the wire, bank said should arrive today.
2024/02/27 08:13:11 David Sham: Okay, keep me posted
2024/02/27 08:13:17 David Sham: BTC already at 56K
2024/02/27 08:13:27 David Sham: The market is on it’s all time high run
2024/02/27 08:13:51 David Sham: Wire is usually same day almost instant. Did you make a mistake with the transaction ?
2024/02/27 08:39:54 8:live:ph2corp_2: I'll contact Support and find out why.
2024/02/27 09:12:13 David Sham: Okay keep me posted
2024/02/27 09:29:24 8:live:ph2corp_2: Crypto Support just told me it can take 1-5 business days to process a wire deposit.
2024/02/27 09:29:51 David Sham: Oh that’s new. Okay lmk once it’s cleared
2024/02/27 10:05:14 8:live:ph2corp_2: Wire has arrived in my account
2024/02/27 10:12:45 8:live:ph2corp_2: $110K deposit cleared and ready to go.
2024/02/27 11:46:44 David Sham: Cool, you can set up a software trading account with https://upwintrade.com
2024/02/27 11:47:43 David Sham: While waiting for your account to get verified you can purchase bitcoin with the money you funded on your crypto.com
2024/02/27 11:49:10 David Sham: Once your account is verify, fund your account with the bitcoin and keep me posted when this is done so we can get started
2024/02/27 11:54:01 David Sham: Are you there ?
2024/02/27 11:55:30 8:live:ph2corp_2: I just signed up and waiting for verification.
How many bitcoins shall I purchase?
2024/02/27 11:58:16 8:live:ph2corp_2: I just purchased 1.9 BTC.
2024/02/27 12:00:01 David Sham: Purchase bitcoin with the whole amount
2024/02/27 12:01:05 8:live:ph2corp_2: I did
2024/02/27 12:02:55 David Sham: Okay keep me posted
2024/02/27 12:04:21 8:live:ph2corp_2: Will do.
2024/02/27 12:09:44 David Sham: Refresh webpage to know if you are verified
2024/02/27 12:10:14 David Sham: Account should verified already
2024/02/27 12:24:30 8:live:ph2corp_2: It's verified. What's next?
2024/02/27 12:34:42 David Sham: You can fund your account by using the bitcoin you purchased on crypto.com
2024/02/27 12:35:12 8:live:ph2corp_2: Can you walk me thru this.
2024/02/27 12:35:21 8:live:ph2corp_2: Can we get on Skype
2024/02/27 12:36:07 David Sham: Trades about to start, can’t get on a call now.
2024/02/27 12:36:19 David Sham: On options menu select fund account
2024/02/27 12:36:29 David Sham: You’ll see your funding Btc wallet address
2024/02/27 12:36:49 David Sham: Transfer Btc from crypto.com
To your upwin account
2024/02/27 12:37:17 David Sham: Do you understand?
2024/02/27 12:38:20 8:live:ph2corp_2: No.
2024/02/27 12:39:00 8:live:ph2corp_2: I whitelisted an address. That's as far as I've gotten.
2024/02/27 12:41:59 8:live:ph2corp_2: I'm stuck, I'll wait for when you can walk me through this. Don't want to make any mistakes.
2024/02/27 12:46:26 David Sham: Did you find your wallet address in upwin ?
2024/02/27 12:47:14 8:live:ph2corp_2: Is that the QR code under Fund Acct?
2024/02/27 12:47:58 David Sham: Yes that’s correct
2024/02/27 12:48:13 8:live:ph2corp_2: Okay what's next?
2024/02/27 12:48:14 David Sham: Send bitcoin from your crypto.com to that address
2024/02/27 12:49:27 8:live:ph2corp_2: Buy sell transfer are my options. Which one?
2024/02/27 12:49:54 David Sham: Transfer
2024/02/27 12:50:44 David Sham: You can also send me screenshot of your page
2024/02/27 12:50:50 8:live:ph2corp_2: Under transfer, it says deposit or withdraw.
Which one?
2024/02/27 12:50:57 David Sham: Withdraw
2024/02/27 12:52:03 8:live:ph2corp_2: Ok. And then External Wallet?
2024/02/27 12:52:28 David Sham: Yes external wallet

Exhibit 1-I

Orlando Bell

Generated by Loni M Harris on Thursday, June 6, 2024 at 12:20 PM UTC-07:00
Contains data you requested from June 6, 2023 at 6:22 AM to June 5, 2024 at 12:11 PM

Loni M Harris

0:02 / 2:13

May 10, 2024 5:00:43pm

Loni M Harris

Orlando missed your call.

May 10, 2024 3:59:59pm

Loni M Harris

On another note how's your project coming along?

May 09, 2024 6:08:33pm

Loni M Harris

Thanks for getting back to me. I really do appreciate it.

There was definitely a learning curve doing our first trade I think we're starting to understand the process

I know we were Just talking about how people are so dishonest. Its awful!! It's happen to our business too so i understand

May 09, 2024 6:08:09pm

Orlando Bell

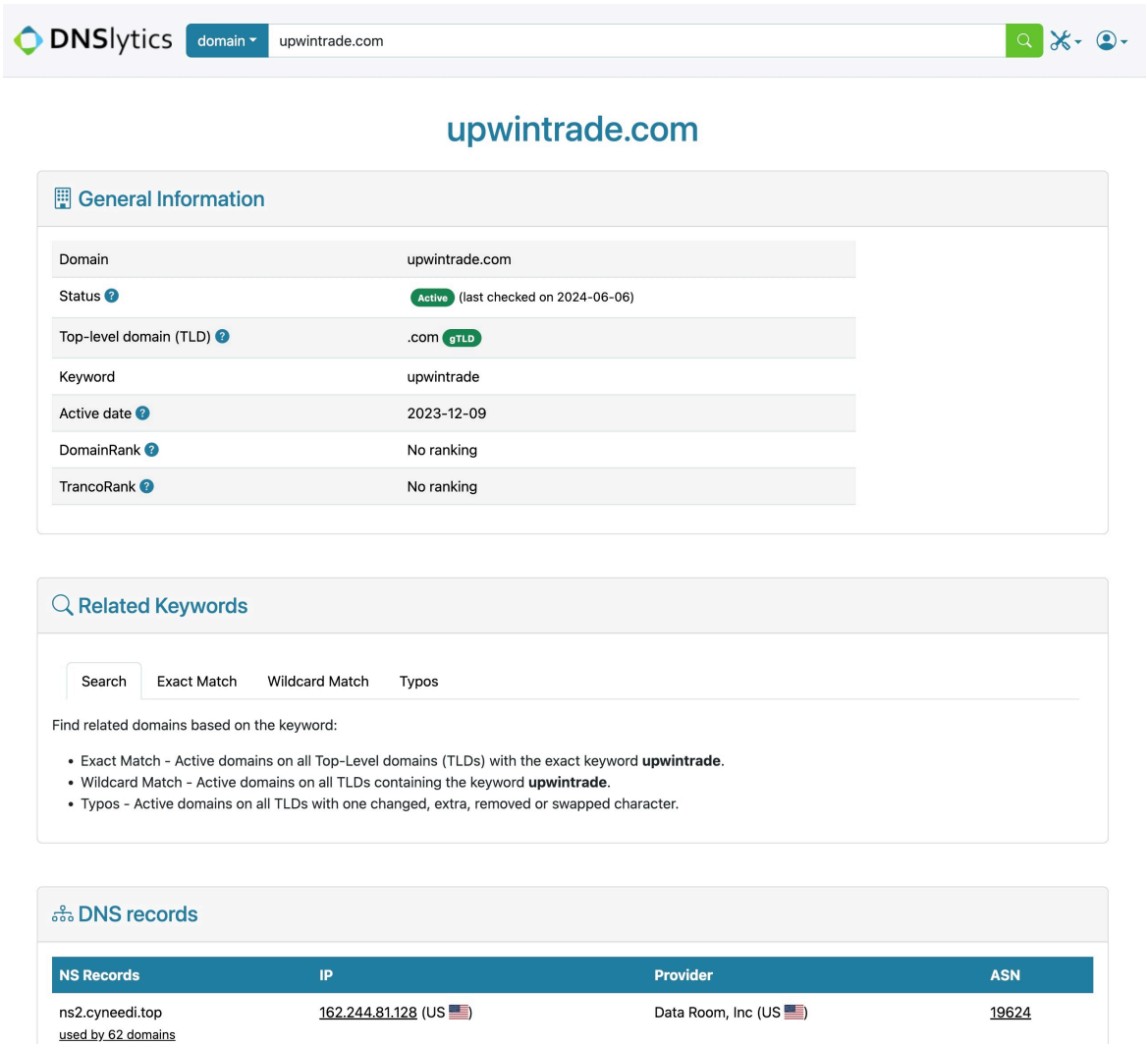
I usually pay him 15% upfront from my pocket, he said they were scammed multiple times, people withdrew an not pay commission. They even block him. I don't know why people will be so greedy to do that to him and his after making money for them.
David is a really awesome person, he works with a bunch of traders which can make it difficult for him to appro your withdrawal without his team. Once you understand the whole process, you won't have to worry about a th

May 09, 2024 5:58:13pm

Loni M Harris

I am sorry I keep bugging you. We are on a time crunch.

Exhibit 1-J


DNSlytics
domain
upwintrade.com
upwintrade.com
General Information
Domain
upwintrade.com
Status
Active
(last checked on 2024-06-06)
Top-level domain (TLD)
.com
gTLD
Keyword
upwintrade
Active date
2023-12-09
DomainRank
No ranking
TrancoRank
No ranking
Related Keywords
Search
Exact Match
Wildcard Match
Typos
Find related domains based on the keyword:
Exact Match - Active domains on all Top-Level domains (TLDs) with the exact keyword upwintrade.
Wildcard Match - Active domains on all TLDs containing the keyword upwintrade.
Typos - Active domains on all TLDs with one changed, extra, removed or swapped character.
DNS records
NS Records
IP
Provider
ASN
ns2.cyneedi.top
used by 62 domains
162.244.81.128 (US
Data Room, Inc (US
19624

- Exact Match - Active domains on all Top-Level domains (TLDs) with the exact keyword **upwintrade**.
- Wildcard Match - Active domains on all TLDs containing the keyword **upwintrade**.
- Typos - Active domains on all TLDs with one changed, extra, removed or swapped character.

DNS records

NS Records	IP	Provider	ASN
ns2.cyneedi.top used by 62 domains	162.244.81.128 (US)	Data Room, Inc (US)	19624
ns1.cyneedi.top used by 62 domains	162.244.81.128 (US)	Data Room, Inc (US)	19624

A/AAAA Records	Provider	ASN
162.244.81.128 (US) used by 62 domains	Data Room, Inc (US)	19624

MX Records	IP	Provider	ASN
upwintrade.com used by 1 domain	162.244.81.128 (US)	Data Room, Inc (US)	19624

SPF record
v=spf1 ip4:162.244.81.128 +a +mx ~all

Last updated on 2024-06-06

Website Information

Website | Redirects

HTTP statuscode	200
HTML Title	Crypto and Stock Trading with Upwin Trade
HTML Description	Being experts in serving institutional and professional clients, Upwin Trade boasts bespoke liquidity pool with best in class connectivity across all asset classes

HTTP statuscode	200
HTML Title	Crypto and Stock Trading with Upwin Trade
HTML Description	Being experts in serving institutional and professional clients, Upwin Trade boasts bespoke liquidity pool with best in class connectivity across all asset classes.
HTML Keywords	

Last updated on 2024-06-15

Whois Information

```
Domain Name: upwintrade.com
Registry Domain ID: 2836104431_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namesrs.com
Registrar URL: https://www.namesrs.com
Creation Date: 2023-12-08T13:20:02.00Z
Registrar Registration Expiration Date: 2024-12-08T13:20:02.00Z
Registrar: Name SRS AB
Registrar IANA ID: 638
Registrar Abuse Contact Email: abuse@namesrs.com
Registrar Abuse Contact Phone: +46.313011220
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: Protected
Registrant Name: Protected Protected
Registrant Organization: Shield Whois
Registrant Street: Radiovägen 2
Registrant City: Västra Frölunda
Registrant State:
Registrant Postal Code: 42147
Registrant Country: SE
Registrant Phone: +46.104500390
Registrant Fax:
Registrant Email: upwintrade.com@shieldwhois.com
Registry Admin ID: Protected
Admin Name: Protected Protected
Admin Organization: Shield Whois
Admin Street: Radiovägen 2
Admin City: Västra Frölunda
Admin Postal Code: 42147
Admin Country: SE
Admin Phone: +46.104500390
Admin Fax:
Admin Email: upwintrade.com@shieldwhois.com
Registry Tech ID: Protected
Tech Name: Protected Protected
Tech Organization: Shield Whois
Tech Street: Radiovägen 2
Tech City: Västra Frölunda
Tech Postal Code: 42147
```

```
Admin Phone: +46.104500390
Admin Fax:
Admin Email: upwintrade.com@shieldwhois.com
Registry Tech ID: Protected
Tech Name: Protected Protected
Tech Organization: Shield Whois
Tech Street: Radiovägen 2
Tech City: Västra Frölunda
Tech Postal Code: 42147
Tech Country: SE
Tech Phone: +46.104500390
Tech Fax:
Tech Email: upwintrade.com@shieldwhois.com
Name Server: NS1.CYNEEDI.TOP
Name Server: NS2.CYNEEDI.TOP
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
Last update of WHOIS database: 2024-06-19T12:59:59.00Z

Whois information protected.
Contact the registrant via http://www.shieldwhois.com

Whois server 3.0

The data in the www.namesrs.com whois database is provided to you for
information purposes only, that is, to assist you in obtaining information
about or related to a domain name registration record. We make this
information available "as is," and do not guarantee its accuracy.

By submitting a whois query, you agree that you will use this data only for
lawful purposes and that, under no circumstances will you use this data to:

(1) enable high volume, automated, electronic processes that stress or load
this whois database system providing you this information; or
(2) allow, enable, or otherwise support the transmission of mass
unsolicited,
commercial advertising or solicitations via direct mail, electronic
mail, or by telephone. The compilation, repackaging, dissemination or
other use of this data is expressly prohibited without prior written
consent from us.

NOTE! ALL WHOIS QUERIES AND IP ADDRESSES ARE LOGGED!
```

Last updated on 2024-06-19

Exhibit 1-K

Home / upwintrade.com Technology Profile / upwintrade.com Detailed Technology Profile

UPWINTRADE.COM

Technology Profile | Detailed Technology Profile | Meta Profile | Performance | Relationship | Redirect | Recommendations | Company

You have used 1 of 10 lookups you can do on a free account currently.

View Plans

Advanced also provides unlimited detailed lookups.

UPWINTRADE.COM

Analytics and Tracking	First Detected	Last Detected	
Akamai mPulse Application Performance	May 2024	Jul 2024	$
Widgets			
Financial Conduct Authority	May 2024	Jul 2024	$
JivoSite Live Chat	May 2024	Jul 2024	$
WPML Multilingual WordPress Plugins	May 2024	Jul 2024	$
Wordpress Plugins	May 2024	Jun 2024	
Frameworks			
CodeIgniter	May 2024	Jun 2024	
Foundation	May 2024	Jun 2024	
Content Delivery Network			
UNPKG	May 2024	Jul 2024	
Akamai	May 2024	Jul 2024	
Mobile			
Apple Mobile Web Clips Icon	May 2024	Jul 2024	
Viewport Meta	May 2024	Jul 2024	
IPhone / Mobile Compatible	May 2024	Jul 2024	
Payment			
MasterCard Payment Acceptance	May 2024	Jun 2024	
Visa Payment Acceptance	May 2024	Jun 2024	
Content Management System			
WordPress Open Source · Blog	May 2024	Jul 2024	
JavaScript Libraries and Functions			
AOS	May 2024	Jul 2024	
jQuery JavaScript Library	May 2024	Jul 2024	
jQuery UI jQuery Plugin · UI	May 2024	Jul 2024	
jQuery Marquee jQuery Plugin	May 2024	Jul 2024	
DataTables jQuery Plugin	May 2024	Jun 2024	
SSL Certificates			
SSL by Default	May 2024	Jun 2024	
LetsEncrypt Root Authority	May 2024	Jun 2024	
Email Hosting Providers			

SPF	May 2024	Jun 2024
Web Servers		
Apache	May 2024	Jun 2024

UPWINTRADE.COM/*

Payment	First Detected	Last Detected
Euro Currency	Jun 2024	Jul 2024

Exhibit 1-L

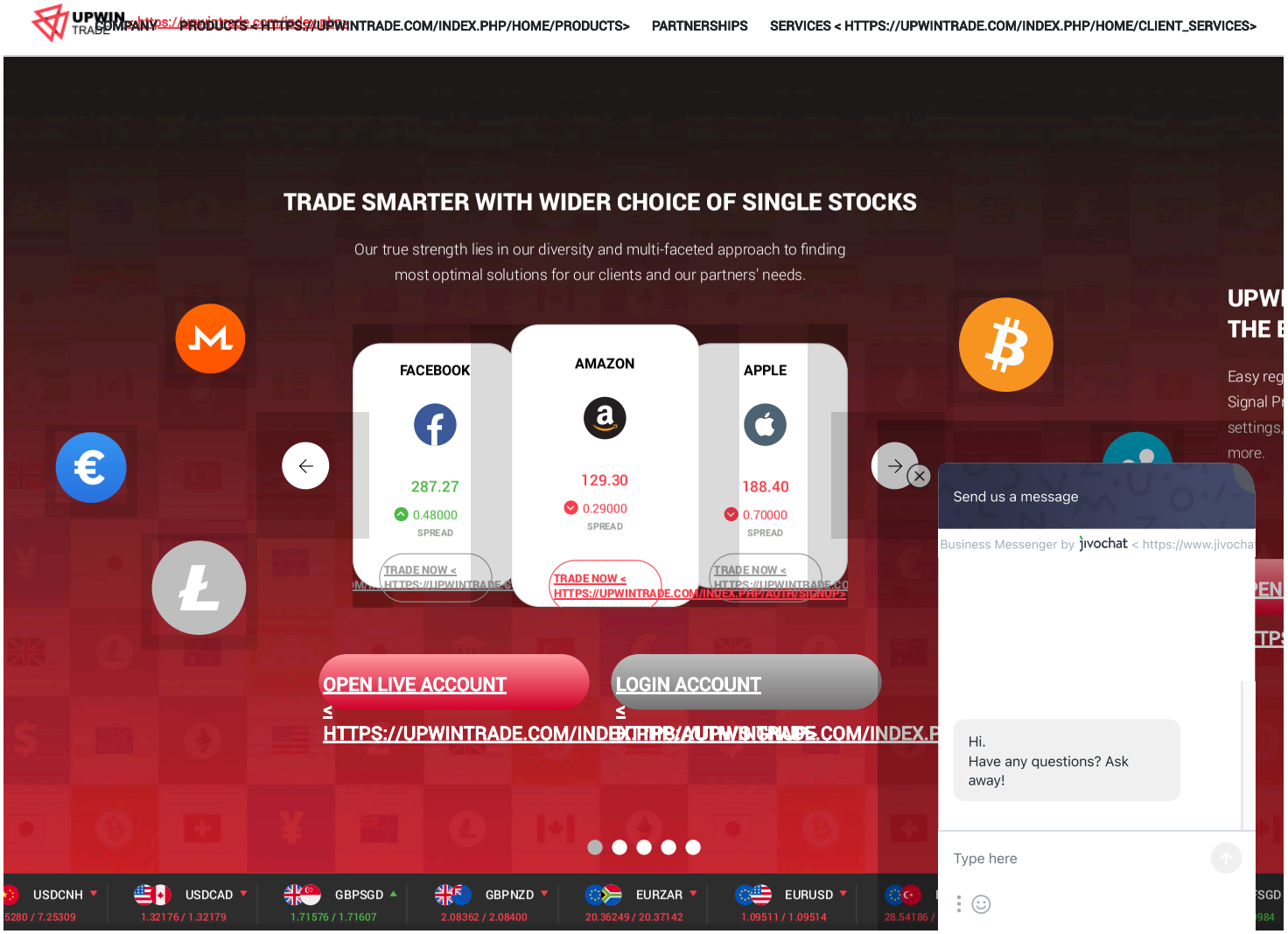
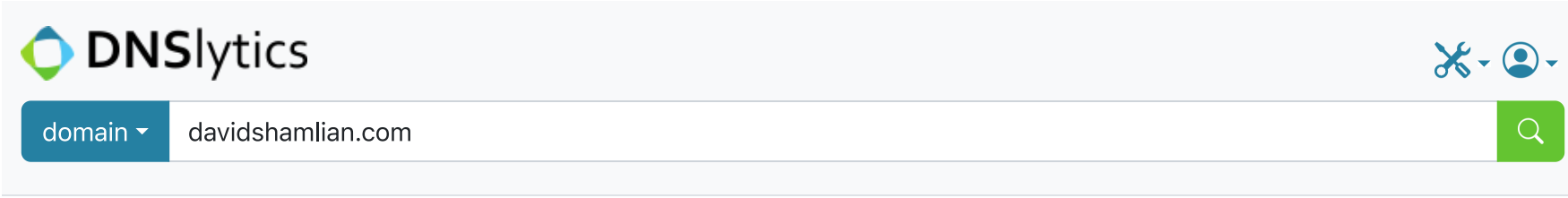


Exhibit 1-M



davidshamlian.com

General Information

Domain	davidshamlian.com
Status	Active (last checked on 2024-07-13)
Top-level domain (TLD)	.com gTLD
Keyword	davidshamlian
Active date	2024-01-10
DomainRank	No ranking
TrancoRank	No ranking

Related Domains

Search | Exact Match | Wildcard Match | Typos

Find related domains based on the keyword:

- Exact Match - Active domains on all Top-Level domains (TLDs) with the exact keyword **davidshamlian**.
- Wildcard Match - Active domains on all TLDs containing the keyword **davidshamlian**.
- Typos - Active domains on all TLDs with one changed, extra, removed or swapped character.

DNS Records

Domain Records | PTR Records

NS Records	IP	Provider	ASN
ns2.orangehost.com used by 20,695 domains	173.252.167.3 (US)	OrangeHost (US)	19853
ns1.orangehost.com used by 20,701 domains	209.172.2.3 (US)	OrangeHost (US)	19853

A/AAAA Records	Provider	ASN
173.252.167.160 (US) used by 563 domains	OrangeHost (US)	19853

MX Records	IP	Provider	ASN
davidshamlian.com used by 1 domain	173.252.167.160 (US)	OrangeHost (US)	19853

SPF record
v=spf1 +a +mx +ip4:173.252.167.160 ~all

Last updated on 2024-07-13

Website Information

Website | Redirects

HTTP statuscode	200
HTML Title	David Shamlian – Crypto Trader
HTML Description	
HTML Keywords	

Last updated on 2024-07-17

Whois Information

```
Domain Name: davidshamlian.com
Registry Domain ID: 2844545195_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.wildwestdomains.com
Registrar URL: https://www.wildwestdomains.com
Updated Date: 2024-01-09T08:01:00Z
Creation Date: 2024-01-09T08:01:00Z
Registrar Registration Expiration Date: 2025-01-09T08:01:00Z
Registrar: Wild West Domains, LLC
Registrar IANA ID: 440
Registrar Abuse Contact Email: abuse@wildwestdomains.com
Registrar Abuse Contact Phone: +1.4806242505
Reseller: OrangeHost
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Registrant Organization: David Shamlian
Registrant State/Province: Arizona
Registrant Country: US
Registrant Email: Select Contact Domain Holder link at https://www.secureserver.net/whois?plid=1387&domain=davidshaml
Admin Email: Select Contact Domain Holder link at https://www.secureserver.net/whois?plid=1387&domain=davidshamlian.c
Tech Email: Select Contact Domain Holder link at https://www.secureserver.net/whois?plid=1387&domain=davidshamlian.co
Name Server: NS1.ORANGEHOST.COM
Name Server: NS2.ORANGEHOST.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2024-07-26T13:57:22Z <<<
For more information on Whois status codes, please visit https://icann.org/epp

TERMS OF USE: The data contained in this registrar's Whois database, while believed by the
registrar to be reliable, is provided "as is" with no guarantee or warranties regarding its
accuracy. This information is provided for the sole purpose of assisting you in obtaining
information about domain name registration records. Any use of this data for any other purpose
is expressly forbidden without the prior written permission of this registrar. By submitting
an inquiry, you agree to these terms and limitations of warranty. In particular, you agree not
```

```
to use this data to allow, enable, or otherwise support the dissemination or collection of this
data, in part or in its entirety, for any purpose, such as transmission by e-mail, telephone,
postal mail, facsimile or other means of mass unsolicited, commercial advertising or solicitations
of any kind, including spam. You further agree not to use this data to enable high volume, automated
or robotic electronic processes designed to collect or compile this data for any purpose, including
mining this data for your own personal or commercial purposes. Failure to comply with these terms
may result in termination of access to the Whois database. These terms may be subject to modification
at any time without notice.
```

Last updated on 2024-07-26

Exhibit 1-N

Home / davidshamlian.com Technology Profile / davidshamlian.com Detailed Technology Profile

DAVIDSHAMLIAN.COM

Technology Profile | Detailed Technology Profile | Meta Profile | Performance | Relationship | Redirect | Recommendations | Company

You have used 2 of 10 lookups you can do on a free account currently.

View Plans

Advanced also provides unlimited detailed lookups.

DAVIDSHAMLIAN.COM

Widgets	First Detected	Last Detected
Redux Framework WordPress Plugins	May 2024	Jun 2024
Contact Form 7 Feedback Forms and Surveys	May 2024	Jun 2024
Google Font API Fonts	May 2024	Jun 2024
Wordpress Plugins	May 2024	May 2024
Elementor WordPress Plugins	May 2024	May 2024
Mobile		
Apple Mobile Web Clips Icon	May 2024	Jun 2024
Viewport Meta	May 2024	Jun 2024
IPhone / Mobile Compatible	May 2024	Jun 2024
Content Delivery Network		
GStatic Google Static Content	May 2024	Jun 2024
Content Management System		
WordPress Open Source · Blog	May 2024	Jun 2024
WordPress 6.5	May 2024	Jun 2024
JavaScript Libraries and Functions		
jQuery JavaScript Library	May 2024	Jun 2024
jQuery UI jQuery Plugin · UI	May 2024	Jun 2024
jQuery 3.7.1	May 2024	Jun 2024
jQuery Waypoints	May 2024	Jun 2024
Slick JS Animation	May 2024	Jun 2024
Magnific Popup	May 2024	Jun 2024
Lightbox	May 2024	Jun 2024
Verified Link		
Facebook	May 2024	Jun 2024
SSL Certificates		
SSL by Default	May 2024	May 2024
LetsEncrypt Root Authority	May 2024	May 2024
Email Hosting Providers		
SPF	May 2024	May 2024
Operating Systems and Servers		
QUIC	May 2024	May 2024
Syndication Techniques		

Really Simple Discovery	May 2024	Jun 2024
RSS	May 2024	Jun 2024